SAFE HARBOR STARTUPS: LIABILITY RULEMAKING UNDER THE DMCA

BRIAN LEARY*

This Note presents two arguments. First, the Digital Millennium Copyright Act's (DMCA) liability safe harbors are inapposite for private cloud services. Private cloud services are increasingly common offerings where consumers upload content, such as music, movies, or books, to personal cloud storage space, then download or stream that content to a multitude of devices. Although granting safe harbor immunity from secondary liability for user infringement would further the DMCA's policy to promote technological innovation, doing so would completely ignore the DMCA's other policy—to protect copyright. Currently, the DMCA protects copyright through its notice-and-takedown procedures, but these provisions depend on the ability of copyright holders to monitor users' public actions—an impossibility on private cloud services. Second, the private cloud services problem is symptomatic of a larger problem in the DMCA: Its regulatory-like detail and specificity undermine its application to new technologies. The solution to both problems is an administrative one: Delegate rulemaking power to narrowly define safe harbor qualification when new technologies, like private cloud services, are valuable but also both ripe for infringement and unaddressed by the DMCA.

 J.D., 2012, New York University School of Law. Many thanks to Michelle Lyon, Nick Walrath, Kade Olsen, Catherine Chu, and the rest of the *New York University Law Review*.

INTRODUCTION

When Sony invented Betamax, Hollywood panicked.[1] Suddenly consumers could record movies and television shows off the air, undermining Hollywood's absolute control over access to content. Universal and Disney sued Sony for copyright infringement,[2] and the Motion Picture Association of America lobbied Congress for new legislation.[3] This is a familiar copyright story: A new technology has valuable, legitimate uses but also facilitates copyright infringement.[4] In the Betamax case, *Sony Corp. of America v. Universal City Studios, Inc.*, the Supreme Court adopted a solution that weighed the value and legitimacy of the new technology against the likely harm to copyright holders.[5] Often, a solution, if only a temporary one, comes from Congress.[6]

---

[1] The president of the Motion Picture Association of America infamously stated before Congress that "the VCR is to the American film producer and the American public as the Boston strangler is to the woman home alone." *Home Recording of Copyrighted Works: Hearings on H.R. 4783, H.R. 4794, H.R. 4808, H.R. 5250, H.R. 5488, and H.R. 5707 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary*, 97th Cong. 8 (1982).

[2] Universal City Studios, Inc. v. Sony Corp. of Am., 480 F. Supp. 429 (C.D. Cal. 1979), *aff'd in part, rev'd in part*, 659 F.2d 963 (9th Cir. 1981), *rev'd*, 464 U.S. 417 (1984); *see infra* Part I.B (discussing *Sony* in greater detail).

[3] The proposed legislation would have required manufacturers of VCRs and blank VHS tapes to pay royalties to the film and television studios. Home Recording Act of 1983, S. 31, 98th Cong. (1983); *see also Video and Audio Home Taping: Hearing on S. 31 and S. 175 Before the Subcomm. on Patents, Copyrights, and Trademarks of the S. Comm. on the Judiciary*, 98th Cong. 276–78 (1983) (statement of Jack Valenti, President, Motion Picture Association of America) (advocating passage of the bill).

[4] For example, the late nineteenth-century development of piano rolls—rolls of perforated paper that control self-playing pianos—threatened the sheet music industry. *See* White-Smith Music Publ'g Co. v. Apollo Co., 209 U.S. 1 (1908) (rejecting a claim that piano rolls infringed the copyright of sheet music). A century later, in the 1990s, the recording industry feared that the ability of digital audio recorders to make perfect copies would undermine CD and cassette tape sales. *See* Niels Schaumann, *Copyright Infringement and Peer-to-Peer Technology*, 28 WM. MITCHELL L. REV. 1001, 1008 (2002) (describing initial industry reactions to digital audio recorders).

[5] Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 440–41 (1984) (importing from patent law a "substantial noninfringing use" doctrine); *see infra* Part I.B (discussing *Sony* in greater detail).

[6] For example, in response to the piano rolls and digital audio recording problems described *supra* note 4, Congress imposed royalties on the respective manufacture of piano rolls and digital audio recorders. Audio Home Recording Act, Pub. L. No. 102-563, 106 Stat. 4237 (1992) (codified at 17 U.S.C. §§ 1001–1010 (2006)); Copyright Act, ch. 320, § 1, 35 Stat. 1075, 1076 (1909). Both legislative and judicial solutions are often spurred by the copyright industries' fear of new technologies. Sometimes these fears are misplaced. *See, e.g.*, Joseph P. Liu, *Regulatory Copyright Law*, 83 N.C. L. REV. 87, 138–39 (2010) (noting that the advent of computers made the fuss and legislation over digital audio recorders largely irrelevant); Stephen Advokat, *Small Screen Begins To Dominate Hollywood Thinking*, ST. PETERSBURG EVENING INDEP., Dec. 26, 1985, at 3-B, *available at*

When this same story began to play out in reaction to the Internet, Congress responded by enacting the Digital Millennium Copyright Act (DMCA).[7] The DMCA has been said to have "saved the Web."[8] By establishing four "safe harbors" to protect legitimate businesses from crippling liability for copyright infringement,[9] the DMCA has enabled innovation online. But promoting innovation is only one of the DMCA's two core goals—it also aims to combat copyright infringement.[10] In this way, the DMCA goes one step beyond the weighing of legitimacy and harm in *Sony*. To combat infringement, it conditions safe harbor immunity on cooperation with copyright holders. The most salient cooperative mechanism, the notice-and-takedown regime,[11] although imperfect,[12] offers copyright holders a

http://news.google.com/newspapers?id=EgIMAAAAIBAJ&sjid=XlkDAAAAIBAJ&pg=6921,2690566 (noting that, by 1985, Hollywood made as much from sales of prerecorded VHS tapes as from sales of movie theater tickets).

[7] Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C.). This Note focuses on Title II of the DMCA, the Online Copyright Infringement Liability Limitation Act. Unless otherwise specified, all references to the DMCA throughout are to Title II. Prior to the DMCA, online companies appeared likely to face liability for contributory infringement. *See* Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1373–75 (1995) (finding that Netcom, an ISP that provided Internet access to the operator of an online bulletin board service, may be liable for infringing content posted by a user to the board); BRUCE A. LEHMAN, INFO. INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 213 (1995), *available at* http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf (recommending that ISPs and other companies be liable for both their own and their users' infringing acts).

[8] David Kravets, *10 Years Later, Misunderstood DMCA Is the Law that Saved the Web*, WIRED: THREAT LEVEL (Oct. 27, 2008, 3:01 PM), http://www.wired.com/threatlevel/2008/10/ten-years-later/. Kravets argues that the wealth of online innovation and the rise of major Internet companies like Google would not have occurred without the DMCA safe harbors. *Id.*

[9] The relevant safe harbors and requirements for qualification are discussed in greater detail in Part I.A, *infra*.

[10] Congress wrote both interests into the legislative history: to promote innovation by providing "greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities" and to provide "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." H.R. REP. NO. 105-796, at 72 (1998) (Conf. Rep.); *accord* H.R. REP. NO. 105-551, pt. 2, at 49–50 (1998); S. REP. NO. 105-190, at 20, 40 (1998). These goals parallel the constitutional directive of copyright law to "promote the Progress of Science"—or, in other words, to advance knowledge and education—"by securing . . . to Authors . . . the exclusive Right to their respective Writings." U.S. CONST. art. I, § 8, cl. 8.

[11] Notice and takedown is defined in 17 U.S.C. § 512(c), (g) (2006) and is discussed further in Part I.A, *infra*.

[12] Two complaints, for example, are that notice and takedown is insensitive to fair use and that it can be abused to suppress speech or to harm competitors. *See, e.g.*, Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, 24 HARV. J.L. & TECH. 171, 177–79 (2010) (summarizing some chilling effects of the notice-and-takedown provisions); *id.* at 216–18, 221–24 (providing

cheap and expedient remedy for individual instances of infringement. But because copyright holders bear the burden of monitoring user activity for infringement,[13] notice and takedown is effective only when user activity is public.

The recent explosive growth of cloud computing[14]—specifically, services offering private space to store, stream, and download content—raises a question unanticipated by the DMCA: Should the safe harbors extend to companies when the nature of their services necessarily precludes monitoring by copyright holders? More broadly, this raises the question of the DMCA's ability to adapt flexibly over time to the same technological innovation it aims to promote.

This Note begins to explore these questions. Part I explores a problem, and Part II posits a solution. Part I argues that private cloud services qualify for safe harbor protection under the text of the DMCA, but that granting such protection would violate the policy balance underlying the DMCA. Whether private cloud services receive DMCA protection is an important question because such services are increasingly common and are likely to grow even more so as part of a consumer paradigm shift from a single personal computer to a multitude of coordinated Internet devices.

Part II argues that the poor fit of the DMCA to private cloud services is symptomatic of the DMCA's inadaptability. The DMCA's regulatory-like specificity and detail provide courts clear guidance in applying the DMCA to circumstances predicted by Congress in 1998, but now constrain courts' ability to adapt the DMCA's underlying

---

examples); CTR. FOR DEMOCRACY & TECH., CAMPAIGN TAKEDOWN TROUBLES: HOW MERITLESS COPYRIGHT CLAIMS THREATEN ONLINE POLITICAL SPEECH (2010), *available at* https://www.cdt.org/files/pdfs/copyright_takedowns.pdf (examining how overly aggressive copyright enforcement by news organizations may impair online political speech). These problems are real, but they are at least cabined by the statute and by the courts. *See* Lenz v. Universal Music Corp., 572 F. Supp. 2d 1150, 1156 (N.D. Cal. 2008) (holding that copyright holders must consider potential fair use before sending takedown notices); § 512(f) (creating liability for damages, including costs and attorneys' fees, for knowingly misrepresenting that material is infringing); Online Policy Grp. v. Diebold, Inc., 337 F. Supp. 2d 1195 (N.D. Cal. 2004) (finding defendant liable under § 512(f)). *But see* Rossi v. Motion Picture Ass'n of Am., 391 F.3d 1000, 1004–05 (9th Cir. 2004) (emphasizing that knowing misrepresentation under § 512(f) is evaluated subjectively, such that merely careless misrepresentations do not create liability).

[13] The policing burden lies on copyright holders because online businesses have no duty under the notice-and-takedown regime until they receive a takedown letter, which must clearly and specifically identify the alleged infringement. Copyright holders are those most likely to send takedown letters. For more details on the notice-and-takedown procedure, see § 512(c)(3) and *infra* Part I.A.2.

[14] Even if used consistently, which it often is not, "cloud computing" is a very broad term. For an introduction and rough definition, see *infra* notes 15–18 and accompanying text.

policy to new technology, such as private cloud services. I advocate embracing the DMCA's regulatory nature: The optimal solution is to revise the DMCA and grant the Librarian of Congress rulemaking authority to extend the safe harbor policies to new technologies.

I
No Safe Harbor for Private Cloud Services

This Note concerns what I refer to as "private cloud services," a particular form of cloud computing. "Cloud computing" lacks a consensus definition[15] but can be roughly summarized as networked access to elastic, pooled computing resources,[16] such as data storage space, server processing power, or remote software applications.[17] Cloud computing, then, is not new: This broad definition describes the earliest mainframe computers and much of the Internet, even from its earliest days.[18]

---

[15] *See, e.g.*, William R. Denny, *Survey of Recent Developments in the Law of Cloud Computing and Software as a Service Agreement*, 66 Bus. Law. 237, 237 (2010) ("[T]here is no uniform definition of cloud computing available."); Mark H. Wittow & Daniel J. Buller, *Cloud Computing: Emerging Legal Issues for Access to Data, Anywhere, Anytime*, 14 J. Internet L. 1, 5 (2010) ("[E]xperts differ on a precise definition of 'cloud computing.'"); Geoffrey A. Fowler & Ben Worthen, *The Internet Industry Is on a Cloud—Whatever That May Mean*, Wall St. J., Mar. 26, 2009, at A1 ("While almost everybody in the tech industry seems to have a cloud-themed project, few agree on the term's definition."); Peter M. Lefkowitz, *Contracting in the Cloud: A Primer*, Bos. Bar J., Summer 2010, at 9, 9 ("[N]o one really can say with precision where the cloud begins and ends.").

The closest to a standardized definition comes from the National Institute of Standards and Technology (NIST) and describes cloud computing broadly: It "enable[s] ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources . . . that can be rapidly provisioned and released with minimal management effort or service provider interaction." Michael Hogan et al., Nat'l Inst. of Standards & Tech., Cloud Computing Standards Roadmap 10, 14 (2011) [hereinafter Cloud Computing Roadmap], *available at* http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909024; *see also, e.g.*, Christopher S. Yoo, *Cloud Computing: Architectural and Policy Implications*, 38 Rev. Indus. Org. 405, 406–09 (2011) (citing the NIST definition). NIST's definition attempts to articulate a full taxonomy of cloud computing, as discussed more fully in notes 16–17, *infra*.

[16] The NIST definition describes network access, rapid elasticity, and resource pooling as three of five common characteristics of cloud computing. Cloud Computing Roadmap, *supra* note 15, at 14. The other two characteristics are on-demand self-service and measured service. *Id.*

[17] The NIST taxonomy details three cloud computing services models, one of which, "Software as a Service," best describes private cloud services. Software as a Service permits consumers "to use the provider's applications running on a cloud infrastructure" and describes, for example, web-based email as well as music lockers. *Id.* at 15.

[18] For example, web-based email services, including early services like Hotmail as well as more recent offerings like Gmail, are cloud-computing services. By comparison, desktop email programs, like Microsoft Outlook, are not. Similarly, photo-sharing sites, like Flickr, and most social networks, like Facebook, are cloud-computing services.

As for private cloud services, the music lockers at issue in *Capitol Records, Inc. v. MP3tunes, LLC* provide an example: A music locker is personal online space to store, stream, and download songs.[19] A user adds to his MP3tunes.com locker by purchasing songs from MP3tunes.com, uploading MP3 files from his personal hard drive, or "sideloading" songs from URLs across the web.[20] A sister search site, Sideload.com, maintains an index of URLs that link to free, downloadable songs.[21] Once a song is added to a user's music locker, that song can be downloaded or streamed (and listened to) from any Internet-connected device on which the appropriate MP3tunes software is installed.[22]

Dropbox is another example of a private cloud service: The service's software automatically syncs files across multiple computers based on the copies stored in a user's private cloud folders.[23] More generally, private cloud services offer private, remote storage space with accompanying software that enables easy uploading, downloading, and streaming of stored content—often content at the core of copyright, such as music, movies, or books.

Private cloud services facilitate copyright infringement because the cloud storage and software combination makes copying files across computers, smartphones, and other devices effortless. When the content copied is under copyright, the act of copying violates the copyright holder's exclusive right of reproduction.[24] Fair use doctrines may protect a user who copies a song from his hard drive into cloud

---

[19] 821 F. Supp. 2d 627, 633 (S.D.N.Y. 2011). *MP3tunes* is one of the first cases to consider private cloud services.

[20] *Id.* at 633–34.

[21] *Id.* at 634. In addition, a user can download and install a Sideload browser plugin that, as she surfs the Web, easily allows her to sideload music files as she comes across them. When a song is sideloaded through the browser plug-in or through manually entered URLs, the hosting URL is added to the Sideload.com index. In this way, the more one user adds to her private locker, the larger the index of songs becomes, and the more other users can add. *Id.*

[22] *Id.* at 633.

[23] More specifically, a Dropbox user downloads and installs software that enables the user to identify files and folders to synchronize with copies stored in the Dropbox cloud service. Users can also upload and download files to the cloud through a web browser. When a user changes a synced file on the computer, the cloud copy is automatically updated; similarly, when a user changes a cloud copy—perhaps through another device—the computer's copy will be updated. For a more detailed description of the service, see *Dropbox Features*, DROPBOX, https://www.dropbox.com/features (last visited Aug. 8, 2012).

[24] *See* 17 U.S.C. § 106(1) (2006) (granting an exclusive right of reproduction). Section 106 also grants exclusive rights to distribute and to publicly perform a work, § 106(3), (4), (6), both of which may be implicated by private cloud services.

storage and then onto his smartphone,[25] but fair use will not excuse a user who uses a private cloud service to share the song with one—or one hundred—of his friends.

Although the users are directly committing the infringing acts when they upload and download copies of copyrighted content, the cloud service provider faces liability under secondary doctrines of contributory[26] and vicarious[27] liability. If the service provider is found liable, it faces outsized statutory damages[28] that could lead to insolvency.[29] On the other hand, if the service provider qualifies for safe harbor protection under the DMCA, the service provider is immune from damages.[30] In other words, applicability of the DMCA can make or break a company,[31] including those offering a private cloud service. Unsurprisingly, then, when Capitol Records, EMI, and fourteen other music companies (collectively, EMI) brought copyright infringement claims against MP3tunes,[32] the case largely turned on whether

[25] Such copying is noncommercial, private, and likely qualifies as space shifting. *See, e.g.*, Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys. Inc., 180 F.3d 1072, 1079 (9th Cir. 1999) (finding that ripping songs from a CD to an MP3 player is permissible fair use). Fair use more generally is too large a concept—and too tangential—to address in this Note in greater detail. For the non-exhaustive statutory guidelines on fair use, see 17 U.S.C. § 107 (2006). *See also* 4 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 13.05 (2012) (providing a more in-depth discussion of fair use).

[26] The service provider would be contributorily liable if the service provider knows, or has reason to know, of the users' direct infringement and "induces, causes or materially contributes to the infringing conduct . . . ." Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971).

[27] The service provider would be vicariously liable if the service provider possesses both the "right and ability to supervise" the infringement and an "obvious and direct financial interest" in the infringement. Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 307 (2d Cir. 1963).

[28] In most cases, copyright owners can opt to forgo actual damages based on lost profits and instead receive statutory damages between $750 and $30,000 per infringed work. 17 U.S.C. § 504(c)(1) (2006).

[29] Because of the potential size of an online company's user base, the number of works infringed by those users can quickly add up. If ten thousand works are at issue—which is not an unreasonable number if, for example, the plaintiffs are a group of music companies—the service provider faces damages between $750,000 and $300 million. If a finding of willful infringement is made, the cap on damages is raised to $150,000 per work. *Id.* at (c)(2). At ten thousand works, then, the potential damages reach $1.5 billion. *E.g.*, Arista Records LLC v. Lime Grp. LLC, 784 F. Supp. 2d 313, 317 (S.D.N.Y. 2011) (noting that potential damages for the ten thousand recordings at issue reached over $1 billion).

[30] *See* 17 U.S.C. § 512(c)(1) (2006) (exempting a service provider from "liab[ility] for monetary relief" due to infringement because of user content); *see also* § 512(a) (no monetary liability for infringement due to automated routing and transmitting content on user request); § 512(b)(1) (no monetary liability for infringement due to caching); § 512(d) (no monetary liability for infringement due to linking).

[31] This makes clear why the DMCA has been called the law that "saved the Web." *Supra* note 8. The DMCA matters in a very real way.

[32] The plaintiffs also brought a direct infringement claim against an MP3tunes executive for his personal infringing acts in using the MP3tunes service. The court granted the

MP3tunes qualified for the DMCA safe harbors.[33]

The remainder of Part I explores this same core question: whether the DMCA should apply to private cloud services. Subpart A looks at the requirements for safe harbor protection under the DMCA and suggests that private cloud services can meet the requirements, at least facially. Indeed, the *MP3tunes* court found the MP3tunes.com service did—generally—qualify for safe harbor immunity.[34] Subpart B, however, distinguishes *MP3tunes* and contends that the DMCA should not extend safe harbor protection to private cloud services. To make this claim, I look both to practical problems resulting from safe harbor protection and to the policy underlying the DMCA.

A. Adhering to the Text of the DMCA

The third DMCA safe harbor, 17 U.S.C. § 512(c), which governs information storage on networks at the direction of users, is most applicable to private cloud services.[35] This user-content safe harbor protects service providers[36] from infringement liability that is "by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service

---

plaintiffs' motion for summary judgment on this claim. Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 649 (S.D.N.Y. 2011).

[33] Absent the DMCA, MP3tunes likely would have been found contributorily liable: MP3tunes provided the site and facility that is the "sole instrumentality of [its] subscribers' infringement" and should have known that its sites would be used to facilitate infringing acts. *Id.* at 648 (quoting Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124, 155 (S.D.N.Y. 2009)) (internal quotation marks omitted); *see also supra* note 26 (quoting elements of contributory liability).

[34] *MP3tunes*, 821 F. Supp. 2d at 650. Although MP3tunes's service generally qualified for safe harbor protection, because the court found that the company failed to fulfill its obligations under the notice-and-takedown provisions, MP3tunes was found liable for some users' infringement. *Id.* at 649; *see also infra* notes 69–73 and accompanying text (discussing more thoroughly MP3tunes's liability for failing to fully comply with the notice-and-takedown provisions).

[35] 17 U.S.C. § 512(c) (2006). Subsections 512(a), (b), and (d) create the other three safe harbors. The first safe harbor, for "transitory . . . communications," protects ISPs and other companies that run or own the various technology conduits through which all the bits of Internet data flow. § 512(a). Roughly, qualification requires that the transmission be automatic, transient, and initiated at the direction of a user. *See id.* (clarifying qualification for the transitory communications safe harbor). The second safe harbor, for "caching," requires, essentially, that the cached copy be automatic, intermediate, and temporary. *See* § 512(b) (clarifying qualification for the caching safe harbor). The fourth safe harbor, for search engines, sets out requirements that mirror those of § 512(c), the safe harbor for user content. *See* § 512(d) (clarifying qualification for the search engine safe harbor); *see also infra* notes 37–40 and accompanying text (relating requirements for the user-content safe harbor).

[36] Operators of private cloud services qualify as service providers under the safe harbor as "provider[s] of online services." § 512(k)(1)(B) (defining "service provider").

provider . . . ."[37] Although the statutory language is limited to storage, courts have read "by reason of" to reach collateral "services, access, and operation of facilities . . . [that] flow from the material's placement on the provider's system or network."[38] Thus, if it otherwise qualified, a music locker service would be protected for streaming and downloading user-stored songs as well as for storing the songs.

To qualify for the § 512(c) safe harbor, a private cloud service provider must meet five statutory requirements.[39] First, the service provider must not interfere with "standard technical measures" that copyright owners use to identify and protect their work.[40] Second, the service provider must "reasonably implement[ ]" a policy that terminates the access or account of repeat infringers.[41] Third, the service provider must not receive direct financial benefit from infringement within its ability and right to control.[42] Fourth, if the service provider has actual knowledge of infringement or is "aware of facts or circumstances from which infringing activity is apparent," then the service provider must act expeditiously to remove or disable access to the infringing content.[43] And fifth, the service provider must implement a notice-and-takedown policy.[44]

These five requirements reveal two primary concerns. One revolves around whether the service provider is offering a legitimate service rather than one that overtly facilitates or directly commercializes copyright infringement.[45] The second is whether the service

---

[37] § 512(c)(1).

[38] Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 527 (S.D.N.Y. 2010), *aff'd in part, vacated in part, rev'd in part*, 676 F.3d 19 (2d Cir. 2012); *see also* UMG Recordings, Inc. v. Veoh Networks, Inc., 620 F. Supp. 2d 1081, 1089 (C.D. Cal. 2008) ("[W]hen copyrighted content is displayed or distributed on Veoh it is 'as a result of' or 'attributable to' the fact that users uploaded the content to Veoh's servers to be accessed by other means."); Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1148 (N.D. Cal. 2008) (finding that "facilitating user access to material on its website" does not disqualify the service provider from the safe harbor).

[39] The first two requirements are threshold requirements applicable to all four DMCA safe harbors. The latter three are specific to the § 512(c) safe harbor (but overlap significantly with the § 512(d) requirements).

[40] § 512(i)(1)(B); *see also* § 512(i)(2) (defining standard technical measures). Standard technical measures include, for example, Digital Rights Management (DRM) software.

[41] § 512(i)(1)(A).

[42] § 512(c)(1)(B).

[43] § 512(c)(1)(A).

[44] § 512(c)(1)(C); *see also* § 512(c)(2)–(3) (detailing requirements of notice and takedown).

[45] Additionally, a service provider will fail to receive DMCA protection if the provider induces user infringement. *See* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 916 (2005) ("[O]ne 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

provider is doing its part to deter infringement.[46] The following two subsections address the five statutory requirements in the context of these two concerns, using *MP3tunes* as an example to consider specific problems implicated by private cloud services.

1. Establishing Legitimacy

Two requirements most directly demonstrate legitimacy. Meeting one—the prohibition on interference with standard technical measures—is easy. Violation requires active interference with anti-infringement technical measures, whereas qualification is met by simply doing nothing.

The other requires that a service provider not "receive a financial benefit directly attributable to the infringing activity . . . [when] the service provider has the right and ability to control such activity."[47] Violation requires more than a mere link between the benefit and infringing activity.[48] The legislative history, for example, states that a "legitimate business" does not receive a direct financial benefit "where the infringer makes the same kind of payment as non-infringing users of the provider's services."[49] And many courts

---

foster infringement, is liable for the resulting acts of infringement by third parties."). As one court has stated:

> [I]nducement liability and the [DMCA] safe harbors are inherently contradictory. Inducement liability is based on active bad faith conduct aimed at promoting infringement; the statutory safe harbors are based on passive good faith conduct aimed at operating a legitimate internet business. . . . Defendants are liable for inducement. There is no safe harbor for such conduct.

Columbia Pictures Indus. Inc. v. Fung, No. CV 06-5578 SSW(JCx), 2009 WL 6355911, at *18 (C.D. Cal. Dec. 21, 2009).

[46] Demonstrating that a service provider cooperates in deterring infringement helps to show the legitimacy of the service. The two inquiries are not statutorily separated, but I present them separately because they help to illuminate the policy goals of the DMCA, as compared to alternate solutions and as discussed further in Part I.B, *infra*.

[47] § 512(c)(1)(B).

[48] For example, it is not enough if infringing uses of a website draw traffic, increasing financial benefits in the form of advertising or user fees. *See* Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 645 (S.D.N.Y. 2011) (rejecting EMI's traffic-draw argument). EMI's traffic-draw argument borrows from case law on vicarious liability, which also requires control and financial benefit. *See, e.g.*, A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001) (finding Napster vicariously liable under a draw theory); *see also supra* note 27 (stating elements of vicarious liability). Even the Ninth Circuit has refused to import its control and financial benefit standard under vicarious liability as in *Napster* to the control and financial benefit standard under the DMCA. *See* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1043–45 (9th Cir. 2011) (examining both the plain language and legislative history of the DMCA to hold that the *Napster* standard is inapplicable under the DMCA).

[49] H.R. REP. NO. 105-551, pt. 2, at 54 (1998); *see also MP3tunes*, 821 F. Supp. 2d at 645 (citing legislative history). MP3tunes, for example, requires all users to pay alike—nothing. *Id.* at 644.

have held that ability to control infringing activity requires item-specific knowledge of it.[50] Ability to control is not met by a general technical ability to block content.[51] The Second Circuit suggests that an ability and right to control may be shown by a "service provider [that] exert[s] substantial influence on the activities of users . . . ."[52] For example, a service provider that imposes a user-monitoring program providing "detailed instructions regard[ing] issues of layout, appearance, and content," forbidding certain types of content, and refusing access to users who do not comply has demonstrated the requisite level of control.[53]

Adherence to these two requirements establishes threshold legitimacy: At the least, the provider's service neither overtly facilitates nor directly commercializes infringement. Nothing inherent in private cloud services would prevent general adherence with these two requirements.

2. Deterring Infringement

The statutory requirements for safe harbor under § 512(c) also show that a service provider must cooperate to deter infringement. The DMCA explicitly disavows any expectation that service providers will actively monitor their users or their service for infringing activity,[54] but the DMCA does impose specific duties in response to claims of infringement.

First, a service provider must have a reasonable repeat infringer policy. Because courts do not require particular formalities[55] and find

---

[50] *See, e.g.*, *UMG Recordings*, 667 F.3d at 1043 ("[T]he 'right and ability to control' under § 512(c) requires control over specific infringing activity the provider knows about."). *But see* Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 36 (2d Cir. 2012) (rejecting a specificity requirement under right and ability to control as redundant with a specificity requirement under actual or red flag knowledge, discussed *infra* notes 59–71 and accompanying text).

[51] "'[C]ontrol of infringing activity' under the DMCA requires something more than the ability to remove or block access to materials posted on a service provider's website." *MP3tunes*, 821 F. Supp. 2d at 645; *see also YouTube*, 676 F.3d at 38 (quoting this passage from *MP3tunes* but refraining from providing an explicit clarification of "something more").

[52] *YouTube*, 676 F.3d at 38.

[53] Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1173 (C.D. Cal. 2002); *see also YouTube*, 676 F.3d at 38 (citing *Cybernet Ventures* as the one example of a court finding that a service provider possesses the requisite right and ability to control under the DMCA).

[54] *See* 17 U.S.C. § 512(m) (2006) ("Nothing in [§ 512] shall be construed as conditioning the applicability of [the safe harbors] on . . . a service provider monitoring its service or affirmatively seeking facts indicating infringing activity . . . .").

[55] The DMCA defines neither "reasonably implemented" nor "repeat infringer." *MP3tunes*, 821 F. Supp. 2d at 636.

policies reasonable "if, under 'appropriate circumstances,' the service provider terminates users who repeatedly or blatantly infringe copyright,"[56] private cloud services can adopt a variety of repeat infringer policies. EMI argued, for example, that MP3tunes failed to effectuate a reasonable policy because many of its users had sideloaded multiple infringing songs.[57] The court disagreed, distinguishing between users who blatantly upload content for others to download and users, like MP3tunes's, that sideload content for personal use without realizing that their actions violate copyright.[58] Similarly, a video-sharing site has reasonably implemented a repeat infringer policy when the operator terminates the accounts of users who, despite prior warnings, continue to upload infringing material.[59] By comparison, a peer-to-peer network fails to implement a reasonable policy when it encrypts user activity so thoroughly that tracking repeat infringers becomes impossible.[60]

Second, when a service provider possesses actual or red flag knowledge of infringement, it must "act[ ] expeditiously to remove, or disable access to, the [infringing] material."[61] A service provider possesses red flag knowledge when "aware of facts or circumstances from which infringing activity is apparent."[62] The Second Circuit distinguishes red flag from actual knowledge as an objective rather than a subjective inquiry: "[T]he red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement 'objectively' obvious to a reasonable person."[63] Courts have set the red flag threshold very high.[64] A red flag must be "an immense crimson banner" to require any action from service providers.[65]

---

[56] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1109 (9th Cir. 2007).

[57] *MP3tunes*, 821 F. Supp. 2d at 636.

[58] *Id.* at 638. The court also noted that MP3tunes had terminated the accounts of 153 repeat infringers for sharing the content of their music lockers with other users. *Id.* at 637.

[59] UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1117–18 (C.D. Cal. 2009), *aff'd sub nom.* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011).

[60] *In re* Aimster Copyright Litig., 252 F. Supp. 2d 634, 659 (N.D. Ill. 2002), *aff'd*, 334 F.3d 643 (7th Cir. 2003). Private cloud service providers may encounter tension between the requirements of the repeat infringer policy and their users' interests in privacy, but this is a complex issue beyond the scope of this Note.

[61] 17 U.S.C. § 512(c)(1)(A)(iii) (2006).

[62] *Id.* § 512(c)(1)(A)(ii).

[63] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2d Cir. 2012).

[64] *See, e.g.*, *UMG Recordings*, 665 F. Supp. 2d at 1110 (describing the "high bar" of the red flag standard).

[65] 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, 596 (2008).

In the case of private cloud services, content owners may argue that the ease of infringement on such services—and the subsequent reasonable inference of likely generalized widespread infringement—constitutes a red flag.[66] But courts have repeatedly rejected this claim:[67] Red flag knowledge must be of "specific and identifiable infringements of particular individual items";[68] general awareness of even "rampant" infringement is not a red flag.[69] To impose liability for general knowledge would force service providers to police their users' activities, "contraven[ing] the structure and operation of the DMCA."[70] Thus, EMI's allegation that MP3tunes knew of "widespread infringement" on MP3tunes.com and Sideload.com, even if true, failed to qualify as red flag knowledge.[71]

Third, a service provider must abide by the notice-and-takedown provisions. In reality, the most likely means by which a service provider will possess knowledge of infringement is through receipt of a takedown notice. Thus, the most salient anti-infringement behavior from service providers is compliance with notice and takedown. A takedown notice is a letter sent from the copyright owner to the service provider that identifies the copyrighted work, the specific infringing material on the service provider's system, and "information reasonably sufficient to permit the service provider to locate the mate-

---

66 Alternatively, content owners could argue that private cloud service providers are willfully blind to the infringement on their site. The Second Circuit has held that a willful blindness inquiry is appropriate under the knowledge requirement of the DMCA. *YouTube*, 676 F.3d at 38 (finding that the DMCA "does not abrogate" the common law willful blindness doctrine). But the court did not clarify what suffices as willful blindness under the DMCA and only noted that it is limited by the DMCA's § 512(m) express disavowal of an affirmative duty to monitor. *Id.* The court quotes a Seventh Circuit case in which willful blindness was found when a peer-to-peer operator encrypted its network such that it could not obtain any knowledge of specific user activity. *Id.* at 34 (quoting *In re* Aimster Copyright Litig., 334 F.3d 643, 650 (7th Cir. 2003)).

67 Most recently, the Second Circuit rejected a "proposition . . . that the red flag provision 'requires less specificity' than the actual knowledge provision" and noted that "no court has embraced [that] proposition." *YouTube*, 676 F.3d at 32.

68 Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 523 (S.D.N.Y. 2010), *aff'd in part, vacated in part, rev'd in part*, 676 F.3d 19 (2d Cir. 2012); *see also* UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1108 (C.D. Cal. 2009) ("[I]f investigation of 'facts and circumstances' is required to identify material as infringing, then those facts and circumstances are not 'red flags.'"); Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1108 (W.D. Wash. 2004) (distinguishing between general and specific awareness of infringement).

69 Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 644 (S.D.N.Y. 2011) (citing *YouTube*, 718 F. Supp. 2d at 523).

70 *YouTube*, 718 F. Supp. 2d at 523. The *YouTube* court justified the general/specific distinction as "consistent with an area of the law devoted to protection of distinctive individual works, not of libraries." *Id.*

71 *MP3tunes*, 821 F. Supp. 2d at 636.

rial."[72] To maintain DMCA protection, a service provider must publicly designate an agent to receive takedown letters and must, upon receipt of a valid takedown notice, "expeditiously . . . remove, or disable access to," the infringing material.[73]

Private cloud services can generally abide by notice and takedown with little effort. Because of their private nature, private cloud service providers may rarely receive takedown letters, but the DMCA does not deny safe harbor to a service provider that never receives a takedown letter. For most private cloud services, the entire extent of their burden under the notice-and-takedown requirements would be the designation of an agent.

Prior to filing the *MP3tunes* suit, two EMI subsidiaries sent takedown notices to MP3tunes identifying at least 350 song titles and URLs indexed in Sideload.com that linked to sites infringing EMI's copyrights.[74] MP3tunes removed from Sideload.com the URLs identified by EMI but did not remove copies of those songs from its users' lockers[75]—even when its records showed that the song had been sideloaded into the music locker via the infringing link.[76] MP3tunes argued that the DMCA takedown provisions did not require it to remove those copies because EMI had not identified the specific user lockers that contained infringing copies of the songs; requiring MP3tunes to trace the source of users' copies would require additional searching.[77] The court rejected this argument. Because MP3tunes already tracks the source of each song in each locker, EMI provided sufficient information when it identified specific links on Sideload.com

---

[72] 17 U.S.C. § 512(c)(3) (2006). A valid takedown notice requires additional elements, such as a signature and a statement of good-faith belief in the infringement allegation, *id.*, but the most important are those described above.

[73] § 512(c)(1)(C), (d)(3); *see also* § 512(c)(2) (requiring the designation of an agent to receive notices). The service provider must also "take[ ] reasonable steps" to notify the user who submitted the allegedly infringing material that has been removed or disabled, and that user can serve counter-notice alleging that the material does not infringe. § 512(g)(2); *see also* § 512(g)(3) (outlining counter-notice requirements). In such a circumstance, the service provider must notify the copyright owner who sent the original takedown letter that the material will be placed back online ten to fourteen days after receipt of the counter-notice, unless the copyright owner files an action in court. § 512(g)(2)(B).

[74] *MP3tunes*, 821 F. Supp. 2d at 635. The takedown letters also included a list of EMI artists and a general demand that MP3tunes "remove all of EMI's copyrighted works, even those not specifically identified." *Id.* The list of songs and URLs met the requirements of the takedown provision, but the second general demand did not because it failed to sufficiently identify the specific infringing material and its location on the MP3tunes.com service. *Id.* at 642 (citing UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1109–10 (C.D. Cal. 2009)).

[75] *MP3tunes*, 821 F. Supp. 2d at 635.

[76] *Id.* at 642–43.

[77] *Id.* at 643.

that linked to infringing content. MP3tunes had records of which lockers contained copies of songs downloaded from those infringing links; therefore, no subsequent investigation was required.[78]

MP3tunes, then, presents an instance where the notice-and-takedown provisions function even for private cloud services. Despite my core claim that the DMCA should not reach private cloud services because notice and takedown is inapplicable, *MP3tunes* is a defensible (and distinguishable) opinion because the notices were all based on the public listings on Sideload.com. I argue in the next Subpart that the same result should not occur when a private cloud service is not accompanied by a parallel, public service.

B. Violating the Spirit of the DMCA

With the DMCA safe harbors, Congress intended to provide clear liability rules for online service providers and to promote cooperation between the content and technology industries in combating infringement online.[79] The notice-and-takedown provisions encapsulate this policy balance. The DMCA absolves service providers from any affirmative duty to protect their services from infringing user content,[80] imposing that burden instead on copyright owners; in return, however, service providers must act expeditiously to remove infringing content once notified by a copyright owner.[81] Immunizing technology and telecommunication companies serves the public interest by fostering innovation and furthers the constitutional directive of copyright to promote the progress of knowledge[82]—but the balance it strikes holds only because copyright owners can police the public Internet for infringing user content.

To illustrate the problem, consider two hypothetical services:

> *Case one*. A service—call it ProPlayer—offers consumers private cloud storage. Much like Dropbox's users, ProPlayer's users upload and download files individually or sync batches or folders by installing ProPlayer software. Additionally, ProPlayer's users can install media playback software that will stream any music or video

---

[78] *Id.* at 642–43. This finding precluded MP3tunes from receiving DMCA safe harbor protection as to these infringing songs. The court continued by addressing MP3tunes's liability under secondary liability doctrines. *Id.* at 646–49.

[79] Both interests repeat throughout the legislative reports. *See supra* note 10 (quoting the Conference, Senate, and House Reports).

[80] *See supra* note 54 and accompanying text (describing 17 U.S.C. § 512(m) (2006)).

[81] *See supra* notes 72–73 and accompanying text (describing service provider requirements under the notice-and-takedown procedure).

[82] U.S. CONST. art. I, § 8, cl. 8 (granting Congress the power to "promote the Progress of Science . . . by securing for limited Times to Authors . . . the exclusive Right to their respective Writings").

> file stored in the user's cloud storage space, even if that song or video is not stored locally on the playback device. ProPlayer's only advertisement has been a general, untargeted "Your music, your movies—anywhere" slogan on Facebook and Google. ProPlayer's subscribers all pay a flat five-dollar annual fee. The ProPlayer service has spread through word of mouth among professionals in advertising, consulting, and other white-collar industries where workers travel often. Most ProPlayer users are of the do-good, law-abiding kind, although two percent regularly use the service to infringe copyrights.
>
> *Case two*. CollegeCloud is much like ProPlayer. Only two differences distinguish the services: CollegeCloud, by chance word of mouth, is extremely popular among college and high school students, and seventy percent of CollegeCloud subscribers use the service to infringe copyrights—for example, by sharing their music folders with friends and acquaintances for download.

In most ways, ProPlayer and CollegeCloud are generic private cloud services. Both services could meet the five statutory requirements for the DMCA's § 512(c) safe harbor. Nothing in the DMCA, as written and as currently interpreted, addresses the disparate rates of infringement on the services.[83] The DMCA would not distinguish between the two services. Both, then, would be granted broad immunity, but it is not clear that the law should treat ProPlayer and CollegeCloud alike.

The root of the problem lies in the private nature of the two services. Typically, notice and takedown lowers rates of infringement online. If CollegeCloud and ProPlayer were not private services, copyright owners, such as music companies, could search through the material on CollegeCloud to locate copyrighted content available for download. Once identified, the copyright owners could send CollegeCloud takedown notices for works they wished to see removed. Enough takedown notices would reduce the percentage of infringing activity on CollegeCloud, dampening the appeal of the service to consumers who intend to utilize it in infringing ways. But because of the private aspect of the users' activities, the entire notice-and-takedown procedure is moot, and as a result, the DMCA cannot distinguish between services like CollegeCloud and ProPlayer in any meaningful way.

Because the DMCA treats CollegeCloud and ProPlayer alike, it cannot achieve both its goals. The *MP3tunes* case does not address

---

[83] Although CollegeCloud's operators may know generally that their service frequently enables infringement, as discussed *supra* Part I.A.2, courts continue to reject liability claims based on such general awareness.

this problem. MP3tunes offered a hybrid private-public service in the interdependent MP3tunes.com and Sideload.com sites. Although content owners cannot monitor the songs in users' MP3tunes.com lockers, content owners can monitor the search results in Sideload.com. The court's finding of DMCA protection for MP3tunes is narrowly stated:

> Where service providers such as MP3tunes allow users to search for copyrighted works posted to the [I]nternet and to store those works in private accounts, to qualify for DMCA protection, those service providers must (1) keep track of the source and web address of stored copyrighted material, and (2) take content down when copyright owners identify the infringing sources in otherwise compliant notices.[84]

This description of MP3tunes's responsibilities does not extend to a private cloud service unaccompanied by a Sideload.com-like search engine. If both ProPlayer and CollegeCloud are granted protection under the DMCA, then CollegeCloud would profit from its users' unchecked tortious behavior without legal incentive to combat that infringement. On the other hand, if both services are denied protection under the DMCA (perhaps due to these policy problems), then technological innovation may be hindered because ProPlayer, CollegeCloud, and other private services would face crippling liability for damages.[85] Each of these approaches prioritizes one policy goal over the other; neither balances.

Similar problems—and more—result under the *Sony* doctrine.[86] Denied safe harbor under the DMCA, ProPlayer and CollegeCloud would fall back on *Sony* to avoid liability. In some ways, the *Sony*

---

[84] Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 642 (S.D.N.Y. 2011). Granting MP3tunes DMCA protection comports with the cooperative aim expressed by Congress. Although not every instance of infringement will be stamped out, innovation is protected alongside a cooperative scheme that limits infringement. This cooperative scheme only succeeds because the public nature of the Sideload.com search site enables content providers a limited means to monitor infringement.

[85] *See supra* notes 28–30 and accompanying text for a brief discussion of damages. Even if the DMCA could distinguish the services and granted protection only to ProPlayer, doing so would likely chill innovation. Like other user-content services, frequency of infringement flows from user action. Liability may be as much a consequence of serendipity as of any direct action by the service provider. Unable to predict beforehand whether it will develop into a ProPlayer or a CollegeCloud, a company may avoid developing private cloud services altogether.

[86] Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984). For an introduction to the *Sony* case, see *supra* notes 1–5 and accompanying text. The Seventh Circuit has held that a defendant fails the knowledge prong if shown to be willfully blind to infringement. *See In re* Aimster Copyright Litig., 334 F.3d 643, 653–55 (7th Cir. 2003) (refusing to grant Aimster protection because it deployed encryption on its service in an "ostrich-like refusal to discover the extent to which its system was being used to infringe copyright").

doctrine parallels the DMCA: *Sony* conditions immunity on a lack of actual, specific knowledge of infringement; and it inquires into the legitimacy of the defendant's business by protecting only those technologies "capable of commercially significant noninfringing uses."[87] On its face, this language would seem to treat both ProPlayer and CollegeCloud alike:[88] Both services are equally capable of noninfringing uses of commercial value and thus equally deserving of *Sony* protection. Such an outcome, however, fails to improve on the outcomes under the DMCA as described above because it does not impose any mechanisms or incentives to lessen actual infringement on either ProPlayer or CollegeCloud.

Nor does *Sony*'s policy balancing improve on the DMCA. *Sony*'s motivating policy is to protect new technology against the chilling effect of copyright on corollary industries.[89] To that end, *Sony*'s substantial noninfringing use test weighs the value of the technology against the harm to copyright. As applied to any given case, however, *Sony* furthers only one interest.[90] When the DMCA functions properly, as it does on public sites, it simultaneously promotes both goals. This difference is hugely significant online, where there are uncountable numbers of service providers with some measure of infringing activity on their services.[91]

---

[87] *Sony*, 464 U.S. at 442.

[88] Some courts have interpreted *Sony* to focus on likely potential, rather than actual, uses. *See, e.g.*, A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1020 (9th Cir. 2001) ("The district court improperly confined the use analysis to current uses, ignoring the system's capabilities. Consequently, the district court placed undue weight on the proportion of current infringing use as compared to current and future and noninfringing use." (citation omitted)).

[89] *Sony*, 464 U.S. at 446–47, 450–51.

[90] Such a result is especially troubling given a prominent fact—the absence of an ongoing relationship—distinguishing Sony from ProPlayer, CollegeCloud, and other private cloud services, which some courts have suggested would bar private cloud services from *Sony* protection entirely. *See, e.g.*, Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124, 156 (S.D.N.Y. 2009) ("[A] critical part of the Supreme Court's reasoning in *Sony* . . . [is] that Sony's last meaningful contact with the product or the purchaser was at the point of purchase . . . . [Because] Defendants maintain an ongoing relationship with their users . . . *Sony*'s insulation from contributory liability is inapplicable . . . ." (citing *Sony*, 464 U.S. at 438)); *see also* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 934 (2005) (declining to clarify whether the *Sony* doctrine requires the absence of an ongoing relationship).

[91] This difference is further compounded by language in *Sony* and in Justice Breyer's *Grokster* concurrence suggesting that nine percent of noninfringing use is sufficiently substantial. *See Grokster*, 545 U.S. at 950–52 (Breyer, J., concurring) (citing language from *Sony* to make this claim). On the other hand, the *Sony* Court devoted a considerable portion of its opinion to finding that user time-shifting (recording a televised show to watch once at a later time) constitutes fair use, such that even when the copyright holder has not authorized the recording, the user has not infringed. *Sony*, 464 U.S. at 447–56. This part of

If *Sony*'s noninfringing uses test considers actual—rather than, or in addition to, potential—uses,[92] then *Sony* may distinguish between ProPlayer and CollegeCloud. Although the Court has declined to "give precise content" to the proportion of infringing to noninfringing uses necessary to qualify for the safe harbor,[93] hypothetically the line could fall between CollegeCloud and ProPlayer. This would seem to effectuate the DMCA's goal of deterring infringement as well as promoting innovation. But it is a less sophisticated, less desirable solution. First, ProPlayer is again wholly absolved of any responsibility for the infringing activity on its service. So long as that infringing activity remains comfortably below the *Sony* threshold, ProPlayer has no incentive to help reduce it. In contrast, when the notice-and-takedown provisions of the DMCA properly function, they lessen infringement on all legitimate services, regardless of the substantiality of noninfringement. Second, this reading of *Sony* implicitly imposes a duty on CollegeCloud to monitor and lessen infringement over its service. In this way, *Sony* shifts the burden of identifying and policing infringement onto service providers, whereas the DMCA specifically circumscribes the duties of service providers and places that duty on copyright holders.

These hypothetical applications of *Sony* help illuminate the value of the policy underlying the DMCA's liabilities and burdens. An optimal solution to the private cloud services problem, then, is to modify the DMCA so that its policy can be effectuated properly. As discussed in greater detail in Part II *infra*, an optimal solution would distinguish between ProPlayer and CollegeCloud in a way that protects the legitimate aspects and reduces the illicit uses of each, without significantly altering the burdens established under notice and takedown.

---

the holding was unnecessary if the Court felt that nine percent of authorized time-shifting sufficiently met the substantial noninfringing use test.

[92] Whereas some courts have focused on the "capable" language from *Sony*, *see supra* note 88, others have noted that a mere "*possibility* of substantial noninfringing uses" is insufficient without "any evidence that [a] service has ever been used for a noninfringing use," *In re* Aimster Copyright Litig., 334 F.3d 643, 652 (7th Cir. 2003). Justice Ginsburg endorsed this view of *Sony* in her *Grokster* concurrence. *See Grokster*, 545 U.S. at 948 (Ginsburg, J., concurring) (arguing that any grant of a *Sony* defense based on a product's capacity for noninfringing use requires sound evidentiary support sensitive to the actual proportionality of infringing to noninfringing uses).

[93] *Sony*, 464 U.S. at 442. Nor did the Court provide clarification in *Grokster*. *See Grokster*, 545 U.S. at 934 ("[W]e do not revisit *Sony* . . . to add a more quantified description of the point of balance between protection and commerce when liability rests solely on distribution with knowledge that unlawful use will occur. . . . [We] leave further consideration of the *Sony* rule for a day when that may be required."). *But see supra* note 91 (discussing the analysis of *Sony* in Justice Breyer's *Grokster* concurrence); *supra* note 92 (discussing the analysis of *Sony* in Justice Ginsburg's *Grokster* concurrence).

C. Why the Liability of Private Cloud Services Matters

Like many buzzwords, cloud computing engenders some animus for its faddishness[94] and for lacking definitional clarity.[95] But it names a real trend. By September 2008, sixty-nine percent of Americans had used cloud services—mostly web-based email like Gmail and online photo storage like Flickr.[96] In 2008, Dropbox had two hundred thousand users;[97] by October 2011, Dropbox had forty-five million.[98] And in 2011, Amazon, Google, and Apple all announced private cloud music services akin to MP3tunes's.[99] As data transmission speeds continue to increase and as wired devices continue to proliferate, demand for and use of private cloud services will continue to grow.

And as private cloud services grow, so will copyright infringement over the services. As previously described,[100] consumers can easily use private cloud services to make copies of music, movies, books, and other copyrighted material for friends and acquaintances. Call this a VHS problem.[101] It may seem insignificant relative to other forms of infringement online, such as content copied over peer-to-peer networks between strangers across the globe—call that a Napster

---

[94] *See* Dan Farber, *Oracle's Ellison Nails Cloud Computing*, CNET NEWS (Sept. 26, 2008, 12:09 PM), http://news.cnet.com/8301-13953_3-10052188-80.html ("The computer industry is the only industry that is more fashion-driven than women's fashion. Maybe I'm an idiot, but I have no idea what anyone is talking about. What is it? It's complete gibberish. It's insane. When is this idiocy going to stop?" (quoting Larry Ellison, CEO of Oracle Corp.)).

[95] Its broad definition nearly swallows the Web. *See supra* notes 16–19 and accompanying text (offering some definitions of cloud computing).

[96] John B. Horrigan, *Cloud Computing Gains in Currency*, PEW RESEARCH CENTER (Sept. 12, 2008), http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency. The three most common uses were web-based email, online photo storage, and online applications software, such as Google Documents. *Id.*

[97] Victoria Barret, *Dropbox: The Inside Story of Tech's Hottest Startup*, FORBES (Oct. 18, 2011, 8:30 AM), http://www.forbes.com/sites/victoriabarret/2011/10/18/dropbox-the-inside-story-of-techs-hottest-startup/3/.

[98] Press Release, Dropbox, Dropbox Raises $250 Million in Series B Funding (Oct. 18, 2011), *available at* http://www.dropbox.com/press/20111018.

[99] Jacob Ganz, *Apple Announces iCloud Music Service*, NPR (June 6, 2011, 3:47 PM), http://www.npr.org/blogs/therecord/2011/06/07/137005359/apple-announces-icloud-streaming-music-service.

[100] *See supra* notes 24–25 and accompanying text (discussing infringement on private cloud services).

[101] The problem of infringement over private cloud services seems analogous to the *Sony* case, introduced *supra* notes 1–5. The analogy, however, is imprecise. Infringing copies made via private cloud services are perfect copies, cheaply and quickly made, such that copying can spread to significantly large audiences; Betamax copies, on the other hand, are slow to make and of successively poorer quality. Thus, the risk of infringement over private cloud services is greater than that by VCR.

problem[102]—but it becomes increasingly significant as private cloud services gain more and more users. Moreover, private cloud services can generate a Napster problem as well.[103]

Thus the current situation is one of explosive growth, accompanied by likely widespread copyright infringement but contestable legal liability.[104] Uncertain liability rules may chill valuable innovation.[105] If private cloud services are worth protecting and promoting—and if they are not properly immune from secondary liability under the DMCA—then what means of protection is optimal? This is the question taken up in Part II.

---

[102] The second of two Supreme Court opinions on secondary liability in copyright law, *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005), focused on infringement over peer-to-peer networks.

[103] For example, at one time, the "Dropship" open source code took advantage of Dropbox's storage algorithms to turn Dropbox into a file-sharing network. *See* driverdan, *Dropship*, GITHUB, https://github.com/driverdan/dropship (last visited Aug. 8, 2012) (offering the Dropship code and explaining its functionality). With Dropship, a Dropbox user could obtain the hash identifier (a unique ID number) for any file the user added to Dropbox; other users could then add those same files to their Dropbox accounts via the hash identifier, downloading new copies to their own phones and computers. *Id.* Whereas making copies over Dropbox usually requires sharing folders or accounts, and thereby requires identifying the intended recipient, the hashes from Dropship could be shared with complete strangers by merely posting the hash online or forwarding it through email or Facebook. Dropbox later altered its storage algorithms to prevent Dropship from functioning. *Id.*; Keir Thomas, *Dropship: A File-Sharer's Dream Tool?*, PCWORLD BUS. CTR. (Apr. 26, 2011, 11:57 AM), http://pcworld.com/businesscenter/article/226280/dropbox_a_file_sharers_dream_tool.html.

[104] In this Note, I have argued that private cloud services fit within the text of the DMCA's § 512(c) safe harbor, but such a conclusion does not bar media companies from initiating litigation. When Amazon launched its music service in early 2011, the major music companies stonewalled reporters seeking comment: "We are keeping our legal options open." Ethan Smith, *Amazon in Big Push To Clinch Music Deals*, WALL ST. J., Mar. 31, 2011, at B8, *available at* http://online.wsj.com/article/SB10001424052748704530204576232953460633190.html. Media companies do not possess many methods to combat infringement online. Litigation is one effective means of doing so, even if their victories are relatively few. Indeed, stripped of even the use of notice and takedown as an infringement deterrent, media companies may be more likely to litigate. Nor does the holding in the *MP3tunes* case clearly discourage further litigation on the applicability of the DMCA to private cloud services. *See supra* Part I.B (discussing the limited reach of *MP3tunes*). The solution proposed in Part II provides media companies alternate avenues to combat infringement, without resorting to litigation.

[105] Consider, for example, the recent Ninth Circuit holding that Veoh, a video-sharing site akin to YouTube, qualifies for safe harbor protection under the DMCA. UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011). Although Veoh was vindicated, the years-long battle over its liability drove it to bankruptcy. Daniel Cooper, UMG v. Veoh*: Victory Has Never Been So Pyrrhic*, ENGADGET (Dec. 22, 2011, 1:59 PM), http://www.engadget.com/2011/12/22/umg-v-veoh-victory-has-never-been-so-pyrrhic/.

II
Enacting Safe Harbor Rulemaking

The first American Copyright Act was short. Only three pages long, it entitled authors of "map[s], chart[s], [and] book[s]" a sole right to "print[ ], reprint[ ], publish[ ], and vend[ ]" their work for a limited time[106] on fulfillment of limited conditions,[107] and it established specific penalties for violators of the right.[108] By contrast, current copyright law, Title 17 of the United States Code, is 197 pages long.[109]

As Professor Joseph P. Liu notes, early copyright law can be described under a property model:[110] Legislation was "substantively rather simple," "industry—and technology—neutral," and "relie[d] upon the courts for implementation and further articulation of the property entitlement."[111] But throughout the twentieth century, copyright law became more complex and industry specific, with Congress often delineating the details of a right.[112] Liu describes this form of copyright legislation as a regulatory model.[113] In addition to its detail, complexity, and industry specificity, regulatory copyright both "intervenes far more deeply into the actual structure of copyright markets" and "vests more policymaking power in Congress . . . than [in] the courts."[114]

The DMCA exemplifies regulatory copyright.[115] Not only is it industry-specific in its focus on the Internet, it is also technology-

---

106 Act of May 31, 1790, ch. 15, § 1, 1 Stat. 124, 124 (repealed 1802). The Act granted copyright for a fourteen-year term, with an additional, possible fourteen-year renewal term. *Id.*

107 *See id.* §§ 3–4, 1 Stat. at 125 (requiring the deposit of a copy of the work with the clerk of the district court where the author resides and a copy with the Secretary of State).

108 *See id.* § 2, 1 Stat. at 124–25 (establishing a private cause of action, precise remedies, and a statute of limitations).

109 17 U.S.C. (2006).

110 *See* Liu, *supra* note 6, at 94–96 (describing the simple structure of copyright law from 1790 to 1909).

111 *Id.* at 100.

112 For example, the Code contains specific copyright legislation exclusively for boat hull designs. 17 U.S.C. §§ 1301–1332 (2006). Sections 106 and 114–115 offer very detailed and convoluted rules establishing and governing a digital performance right in sound recordings. 17 U.S.C. §§ 106, 114–115 (2006).

113 *See* Liu, *supra* note 6, at 102–05 (describing characteristics of the regulatory model of copyright legislation); *id.* at 105–25 (detailing specific instances of regulatory copyright law).

114 *Id.* at 104.

115 Liu himself presents the DMCA as one example of regulatory copyright legislation. *See id.* at 122 ("[T]he recent Digital Millennium Copyright Act of 1998 (DMCA) provided a slightly new twist to the [regulatory] approach."). However, whereas I focus this Note on the safe harbor provisions in Title II of the DMCA, Liu focuses on the regulatory nature of the anti-circumvention provisions passed under Title I of the DMCA. *See id.* at 122–24

specific in the narrow scope of each safe harbor: The first two protect automated copying and caching by telecommunications companies necessary to deliver content;[116] the fourth narrowly focuses on online hyperlinks;[117] and the third—of concern in this Note and the broadest of the four—is limited to user-uploaded content.[118] The detail and complexity of the DMCA is clear, for example, in the notice-and-takedown provisions, which detail the service provider's preliminary requirement of appointing and registering an agent,[119] spell out the necessary content of a copyright holder's letter requesting takedown,[120] impose specific duties and deadlines upon receipt of a takedown letter,[121] and construct an elaborate counter-notice process mirroring the preceding steps.[122] The liabilities and burdens under the safe harbors and the notice-and-takedown provisions also supplant judicial policy decisions with a congressional compromise.[123]

Regulatory copyright carries drawbacks. For example, complexity can make provisions opaque and can obscure underlying policy goals; and its detail requires knowledge and expertise of particular industries that Congress likely lacks.[124] More importantly, regulatory copyright suffers from inflexibility: Its complexity is written directly into the statute without any mechanism for alteration.[125] Inflexibility is especially troublesome in industries with rapid changes, such as the

(describing the regulatory nature of the legislation and highlighting its groundbreaking delegation of substantive rulemaking power to the Librarian of Congress); *see also* 17 U.S.C. §§ 1201–1202 (2006) (codifying the anti-circumvention provisions of Title I of the DMCA).

116 17 U.S.C. § 512(a), (b) (2006); *see also supra* note 35 (describing the safe harbors in greater detail).

117 § 512(d); *see also supra* note 35 (describing the safe harbors in greater detail).

118 § 512(c); *see also supra* Part I.A (discussing the third safe harbor in greater detail).

119 § 512(c)(2).

120 *See* § 512(c)(3)(A) (detailing six necessary elements of a takedown letter); *see also* § 512(c)(3)(B)(ii) (imposing duties on a service provider if a received takedown letter is missing the first element but contains the other five).

121 *See* § 512(c)(1)(C) (requiring removal of the allegedly infringing material); § 512(g)(2)(A) (requiring notification to the user who uploaded the material).

122 *See* § 512(g)(2)–(3) (governing counter-notice procedures).

123 *See supra* notes 87–91 and accompanying text (discussing the noninfringing uses exception to secondary liability developed by the Court in Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984)). The difference in policy can be seen in the way application of the *Sony* doctrine prioritizes technological development, in proper circumstances, at the expense of copyright enforcement; on the other hand, application of the DMCA balances, and simultaneously promotes, both. Under *Sony*, if a legitimate technology has substantial noninfringing uses, then infringement is ignored; but under the DMCA, the service provider would be obligated to cooperate in deterring all infringement. The role of the *Sony* doctrine online has been limited because of the DMCA.

124 Liu, *supra* note 6, at 135–37.

125 *Id.* at 138.

Internet, as evidenced by the DMCA's inability to adapt to private cloud services.

Even if repealing regulatory copyright and returning to a simpler property-rights model were ideal,[126] it is extraordinarily unlikely. Thus, for problems like that of private cloud services discussed in Part I, the optimal solution is to embrace the DMCA's regulatory nature and delegate rulemaking authority in order to inject the DMCA with expertise and flexibility.[127] The remainder of Part II advocates such a solution: Subpart A outlines a proposal for safe harbor rulemaking; Subpart B discusses the ongoing YouTube litigation and suggests that safe harbor rulemaking would have provided a better, quicker resolution; and Subpart C considers the public losses if the DMCA is not revised and industry players are forced to self-help.

A. Safe Harbor Rulemaking

An optimal solution for private cloud services should reinforce the twin goals animating the DMCA. The solution should clarify liability in order to promote innovation, and it should combat infringement through a cooperative scheme akin to notice and take-

---

[126] Liu's analysis finds that "a more modest, open-ended entitlement structure would be preferable where an industry is new, and technology and the market are still evolving." *Id.* at 144.

[127] Since the DMCA is generally considered a success, Congress may have little incentive to revise it. So why advocate that Congress do so? The recent fuss over the Stop Online Privacy Act (SOPA), H.R. 3261, 112th Cong. (2011), demonstrates two things. *See also* PROTECT IP Act, S. 968, 112th Cong. (2011) (similar legislation proposed in the Senate); Combating Online Infringement and Counterfeits Act, S. 3804, 111th Cong. (2010) (version proposed in previous Senate session). First, the content industries continue to care a great deal about copyright infringement online, and Congress is amenable to these concerns. The DMCA is not a final solution. Second, the massive public outcry that buried SOPA and the PROTECT IP Act loudly signals that the content industries should adopt a more compromising approach in lobbying for future legislation, adjusting to the concerns of the public and, especially, the technology sector. As one commentator observed:

> Legislation that just weeks ago had overwhelming bipartisan support and had provoked little scrutiny generated a grass-roots coalition on the left and the right. Wikipedia made its English-language content unavailable, replaced with a warning [about SOPA] . . . . Google's home page was scarred by a black swatch . . . . Phone calls and e-mail messages poured in to Congressional offices . . . . One by one, prominent backers of the bills dropped off.

Jonathan Weisman, *Web Rises Up To Deflect Bills Seen as Threat*, N.Y. TIMES, Jan. 19, 2012, at B2; *see also* Editorial, *Beyond SOPA*, N.Y. TIMES, Jan. 29, 2012, at SR10 ("welcom[ing] the collapse" of SOPA and the PROTECT IP Act and discussing the overly aggressive stance the bills took on behalf of copyright holders). Given the DMCA's general popularity, especially among the technology sector, it is a wise place to look for a model of compromise in future legislation.

down.[128] Doing so requires judicially apportioning liabilities and burdens.

A 2010 paper by a working group of twenty copyright scholars and practitioners offers one model for modifying the DMCA safe harbors:[129] creating a fifth safe harbor that protects service providers who voluntarily adopt "reasonable, effective, and commercially available" technology that deters infringement.[130] One problem with this formulation is its open-ended imposition on service providers to determine (under the threat of litigation) whether a technological measure that may deter infringement is a measure that is reasonable, effective, and available.[131]

A better model lies in the notice-and-takedown provisions of the DMCA itself. Notice and takedown is perhaps the ugly duckling of the DMCA: It receives more scholarly criticism than other aspects of the safe harbors,[132] and it is a hassle to both the copyright and technology industries,[133] yet it best encapsulates the policy goals of the DMCA in its balance of liabilities and burdens. The safe harbors provide clear, substantial immunity from liability; and notice and takedown places the large initial burden of monitoring and identifying infringement on copyright holders and imposes on technology companies only specific duties of limited scope in response to takedown letters.

---

[128] *See* H.R. REP. NO. 105-796, at 72 (1998) (Conf. Rep.) (expressing congressional intent to promote innovation and cooperation); H.R. REP. NO. 105-551, pt. 2, 49–50 (1998) (same); S. REP. NO. 105-190, at 20, 40 (1998) (same). For quoted language from the congressional reports, see *supra* note 10.

[129] *See* Pamela Samuelson et al., *The Copyright Principles Project: Directions for Reform*, 25 BERKELEY TECH. L.J. 1175, 1180 (2010) (naming the twenty working group participants).

[130] *Id.* at 1217. The paper's discussion of revising the safe harbors is wide-ranging but brief at approximately four pages, *id.* at 1216–20, and thus necessarily limited in detail. It raises a handful of important, unanswered questions. Among the open questions raised by the working group are: first, how to ensure that only reasonable deterrent measures are adopted, *id.* at 1217–18; second, whether a fifth safe harbor should be limited to peer-to-peer networks and to video-sharing sites or applied more broadly, *id.* at 1218–19; and third, whether adoption of deterrent technologies should be optional or mandatory, *id.* at 1219–20. The key aspect of the safe harbor revisions advocated in this Note is rulemaking, which would resolve the first two questions: the regulatory agency evaluates the reasonableness of deterrent measures; and successive rulings can address peer-to-peer networks, video-sharing sites, and many other online technologies. For a discussion of the third question, see *infra* note 137.

[131] The working group recognized this problem and considered that a solution could be to delegate authority to an administrative agency. Samuelson et al., *supra* note 129, at 1217–18. However, because the group could not reach consensus on an administrative solution, *id.* at 1217, they did not develop this idea as thoroughly as this Note does.

[132] For a brief introduction to criticisms of the notice-and-takedown provisions, see *supra* note 12.

[133] *See infra* notes 155–57 and accompanying text (describing complaints by copyright holders that notice and takedown is a futile game of Whac-A-Mole).

My proposal would modify the DMCA to extend liability immunity only to user-content service providers who comply with safe harbor rulemaking[134] and would delegate power to the Librarian of Congress,[135] with the advice of the Copyright Office,[136] to issue periodic rules approving and requiring the implementation of specific anti-infringement measures—substitutes for notice and takedown.[137] This proposal improves the status quo in a handful of key ways. First, it injects flexibility into the DMCA. Second, it relies on and furthers the expertise of the Copyright Office.[138] Given the trend of copyright

---

134 I do not intend in this Note to write specific statutory provisions for modifying the DMCA's safe harbors. However, it seems clear that safe harbor rulemaking would be most effective if it applied even to service providers currently receiving safe harbor protection. To that end, § 512(c)—and perhaps also § 512(d)—would be modified to condition safe harbor immunity on compliance with safe harbor rulemaking.

135 Although the Librarian of Congress does not possess specific expertise in copyright, formally delegating rulemaking authority to the Librarian of Congress rather than the Copyright Office sidesteps concerns that the Copyright Office, as an arm of Congress, cannot constitutionally receive regulatory power. *See, e.g.*, JeanAne Marie Jiles, Note, *Copyright Protection in the New Millennium: Amending the Digital Millennium Copyright Act To Prevent Constitutional Challenges*, 52 ADMIN. L. REV. 443, 454–55 (2000) (considering the potential unconstitutionality of the current DMCA delegation of rulemaking power on anti-circumvention). Because the Librarian of Congress is appointed by the President, subject to the advice and consent of the Senate, 2 U.S.C. § 136 (2006), the Librarian may qualify as an "officer of the United States" under Article II of the Constitution and so may exercise regulatory authority. *See also, e.g.*, *infra* note 138 (discussing rulemaking power already delegated to the Librarian of Congress). The role of the Copyright Office, at least formally, is to lend its expertise and advice to the Librarian.

136 The Copyright Office's primary responsibilities are to maintain records of copyright registration and copyright laws, to gather deposit copies of works for inclusion in the collection of the Library of Congress, and to provide its expert advice to Congress and the executive branch. For a more detailed description of the Copyright Office's general and specific duties, see *United States Copyright Office: A Brief Introduction and History*, U.S. COPYRIGHT OFFICE, http://www.copyright.gov/circs/circ1a.html (last visited Aug. 8, 2012).

137 Some members of the working group advocated making implementation of anti-infringement measures mandatory. *See* Samuelson et al., *supra* note 129, at 1219 ("[T]he law should simply require the deployment of reasonable measures as part of online service systems that create the danger (and fact) of widespread, consumptive copyright infringement."). A better approach is to mimic the current safe harbors under the DMCA: Implementation of approved anti-infringement measures is required to receive safe harbor immunity, but failure to implement has no direct consequences. *See supra* notes 26–33 and accompanying text (discussing the role of the DMCA in relation to liability).

138 One advantage of regulation is the greater expertise brought to an issue by the regulatory agency. *See, e.g.*, Liu, *supra* note 6, at 148 ("A traditional justification for agency involvement has been the greater expertise that an agency can bring to bear on a complex issue."); *supra* note 124 and accompanying text (noting that Congress may lack the knowledge and expertise necessary to legislate copyright law). Although the Librarian of Congress and the Copyright Office are less experienced with regulatory authority than are traditional administrative agencies, the Librarian already possesses very limited rulemaking authority under another provision of the DMCA. *See* 17 U.S.C. § 1201(a)(1) (2006) (delegating rulemaking authority to the Librarian of Congress, "upon the recommendation of the Register of Copyrights," to issue exemptions to a prohibition on anti-circumvention); Arielle Singh, Note, *Agency Regulation in Copyright Law: Rulemaking*

legislation toward regulatory law, it is preferable to invest in the development of an agency with broad copyright expertise. Regular rulemaking will also lead to the development of economic and technological expertise within the Copyright Office—both through experience and hiring. Third, this proposal honors the policy balance of the DMCA. It maintains the same broad grant of liability immunity, and it also places on copyright holders the heaviest burden of developing or identifying anti-infringement measures and of meeting some threshold of proof in front of the Copyright Office before new measures are approved and adopted.

The first duty tasked to the Copyright Office, then, would be determining the particular qualifications necessary for approval of new measures. The revised statute would offer generalized guidelines: For example, the measure should be reasonable, effective, and available.[139] These guidelines would require that a measure be developed and immediately deployable upon release of a ruling[140] and that installation and maintenance of a new measure be deemed cost effective when weighed against its marginal deterrent effect (compared, for example, to notice and takedown).

More specific qualifications would also address the permissible scope of new measures. For example, a new measure may properly target only private music lockers, like those in *MP3tunes*, or may be limited to user-uploaded video sites like YouTube—an example explored in greater detail in Subpart II.B.2 below. Focusing on anti-infringement measures of a narrower scope allows safe harbor rulemaking to better address previously unforeseen technology, like private cloud services, and to better focus the cost-benefit nature of the reasonableness-effectiveness evaluation.[141]

Under the DMCA and Its Broader Implications, 26 BERKELEY TECH. L.J. 527 (2011) (noting that the Librarian of Congress and the Copyright Office have become increasingly sophisticated and effective in their rulemaking). The Copyright Office is also preferable because of its established directive to represent the public interest in copyright matters—an interest that would otherwise be underrepresented in the notice-and-comment stage of safe harbor rulemaking.

[139] *See* Samuelson et al., *supra* note 129, at 1217 (describing reasonableness, effectiveness, and availability requirements).

[140] The working group would require that a new measure be "designed in the first instance to prevent infringement." *Id.* at 1217. But this is unnecessarily narrow: A new measure could also be effectively adopted from preexisting technology. The importance of the availability rule is that it prevents abuse of the rulemaking opportunity to shift the burden of developing anti-infringement measures onto service providers.

[141] Approving deterrent measures of a narrower scope also lessens the burden on service providers to coordinate multiple overlapping measures or to constantly update or install new ones.

Most importantly, specific qualifications would ensure that new anti-infringement measures mimicked the cooperative procedural scheme of notice and takedown. Under notice and takedown, copyright holders self-select their works to be protected by sending individual takedown letters; new measures similarly should require that copyright holders self-select the works to be protected. Additionally, new measures must include a clear mechanism for dispute: Individuals flagged for infringing activity should be able to contest the accusation and should be able to learn the procedures for doing so with reasonable effort. And if an individual does contest the classification of an action as infringement, the measure should default against the copyright holder but provide the copyright holder with the necessary information to file a court action if the copyright holder wishes to do so.[142]

New measures do not need to be technological measures; they could be more procedural and non-technological, like notice and takedown itself. The goal is to provide the content industry with a more flexible avenue to combat infringement—one that honors the policy balance of the DMCA and the notice-and-takedown scheme while improving on the latter's inefficiencies and scalability problems. More effective measures may take many forms. The next Subpart considers an example.

B. Lessons from YouTube

Viacom and YouTube have been tangling over YouTube's liability for copyright-infringing, user-submitted videos since early 2007.[143] The case raises many issues that parallel the private cloud services problem—such as massive damages, questionable qualification under the DMCA, and the scalability problem of notice and takedown. In this Subpart, I contend that safe harbor rulemaking would have better addressed the dispute in the *YouTube* litigation. The first section covers the major facts and issues of the case, and the second presents a counter-history under safe harbor rulemaking.

1. Viacom v. YouTube*: Litigating Red Flag Knowledge*

In March 2007, Viacom sued YouTube, asserting that YouTube should be held secondarily liable for infringing videos uploaded by its

---

142 Notice and takedown, for example, provides these procedures for dispute in the counter-notice regime defined in 17 U.S.C. § 512(g)(3) (2006).

143 Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010), *aff'd in part, vacated in part, rev'd in part*, 676 F.3d 19 (2d Cir. 2012); *see also* Viacom v. YouTube, ELEC. FRONTIER FOUND., https://www.eff.org/cases/viacom-v-youtube (last visited Aug. 8, 2012) (providing an overview of the litigation).

users.[144] Legally, the dispute focuses on whether YouTube should be granted the user-content safe harbor under the DMCA.[145]

Viacom's primary contention is that YouTube, from the beginning, possessed sufficient knowledge of the infringing uses of its site to constitute red flag knowledge.[146] If it did possess such knowledge, then it should have removed the infringing content expeditiously. Because YouTube did not do so, proof of such knowledge would disqualify it from DMCA protection and expose it to secondary liability.[147] The district court and the circuit court acknowledged that "[a] jury could find that the defendants not only were generally aware of, but welcomed, copyright-infringing material being placed on their website."[148] Nevertheless, both courts held that general awareness did not disqualify YouTube from DMCA safe harbor protection.[149]

Viacom's frustration in the face of such findings is understandable. Although the Second Circuit vacated the district court's grant of summary judgment for YouTube,[150] Viacom did not really "win." An alternate holding on this general awareness issue would have better vindicated Viacom's interests by shifting the legal standards of the DMCA in favor of content owners—and thereby dramatically undermining the availability of DMCA protection for private cloud services.

The Second Circuit has remanded the case to the district court for decision.[151] On remand, the district court is instructed to evaluate the sufficiency of Viacom's evidence that YouTube was objectively aware of specific instances of infringement,[152] whether YouTube was willfully

---

144 *YouTube*, 718 F. Supp. 2d at 516.

145 *See id.* (stating that YouTube moved for summary judgment based on the safe harbor protection provided by 17 U.S.C. § 512(c) (2006)).

146 Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 30 (2d Cir. 2012); *YouTube*, 718 F. Supp. 2d at 518–19; *see also supra* Part I.A.2 (discussing red flag knowledge under the DMCA).

147 *See supra* notes 26–33 and accompanying text (briefly summarizing the interplay between the DMCA safe harbors and traditional secondary liability).

148 *YouTube*, 676 F.3d at 33 (quoting *YouTube*, 718 F. Supp. 2d at 518).

149 *YouTube*, 676 F.3d at 26; *YouTube*, 718 F. Supp. 2d at 523. The Ninth Circuit also endorses this interpretation of the DMCA. *See* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1036–37 (9th Cir. 2011) (rejecting DMCA disqualification based on general knowledge).

150 *YouTube*, 676 F.3d at 26.

151 *Id.* at 41–42.

152 *Id.* at 34. Viacom's strongest case on remand may rest on evidence of the YouTube founders' awareness of specific videos that were likely infringing copyright. The Second Circuit cites three pieces of evidence that suggest sufficient knowledge in regard to specific video clips, and naturally each piece of evidence only references a finite number of clips. *See id.* at 32–34 (discussing the evidence in greater detail). Thus, the final result may be that Viacom successfully procures damages from YouTube, but it seems unlikely that such damages would be sufficient to justify the time and cost of five years of litigation.

blind to infringement,[153] and whether YouTube possessed an ability and right to control the infringing activities.[154]

2. *Safe Harbor Rulemaking and Audible Magic as an Alternate Ending*

At the core of the *YouTube* dispute is frustration over the inequity that allows service providers to turn their backs on widespread infringement, leaving copyright holders one inefficient remedy—sending endless takedown letters. Notice and takedown may be pitch-perfect in its policy balance, but its procedures have not scaled alongside the Internet's growth. Content owners describe it as a Sisyphean game of Whac-A-Mole.[155] The sheer quantity of infringement online renders issuing all the necessary notices impossible;[156] as soon as a takedown notice leads to removal of infringing content, "some other 14-year old post[s] the exact same *Simpsons* clip."[157] As enacted, the notice-and-takedown provisions simply failed to predict the sheer quantity of media online fourteen years later. This is another symptomatic drawback of the regulatory-like specificity of the DMCA, but one that safe harbor rulemaking could resolve.

Notice and takedown correctly recognizes that copyright holders best know whether content is copyrighted, whether its use is without permission,[158] and, due to their greater expertise in making fair-use and other nuanced copyright judgments, whether a particular act is infringing. This is especially important because the very core of copyright is a constitutional directive to "promote the Progress" of knowledge and learning:[159] Copyright balances the holder's monopoly entitlement against the public's interest in dissemination and distribution. Contrarily, the best rationale for imposing a duty to monitor on service providers is that service providers can marshal the very

---

153 *Id.* at 35; *see also supra* note 66 (describing the court's willful blindness holding).

154 *YouTube*, 676 F.3d at 36; *see also supra* notes 51–53 and accompanying text (describing the right and ability to control, as discussed by the *YouTube* court).

155 Nate Anderson, *Rightsholders Tire of Takedown Whac-A-Mole, Seek Gov't Help*, ARS TECHNICA (May 4, 2010, 9:05 AM), http://arstechnica.com/tech-policy/news/2010/05/rightsholders-tire-of-takedown-whac-a-mole-seek-govt-help.ars.

156 *Id.*

157 *Id.*

158 Many instances of would-be infringement are permissible due to express licensing. Additionally, copyright holders often *want* their content to be infringed so that it can be seen and distributed. This is true of even large media companies. YouTube emphasizes this point in its briefs: Even Viacom has trouble distinguishing among the videos it posts to YouTube, the infringing videos it wants removed from YouTube, and the infringing videos it would prefer to remain on YouTube. Brief for the Defendants-Appellees at 52, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012) (No. 10-3270).

159 U.S. CONST. art. I, § 8, cl. 8.

technologies of a service that enable infringement to help monitor infringement. One great value of safe harbor rulemaking is that it harnesses that technological expertise by encouraging copyright holders to invest in technological substitutes for notice and takedown.

The *YouTube* case focuses only on the company's early years because, in 2007, YouTube began implementing Content ID,[160] which is proprietary video-filtering software that "compare[s] videos uploaded to YouTube against . . . reference files" provided by copyright holders.[161] Copyright holders can submit their videos and sound recordings to Content ID, and Content ID will block duplicates from being posted to YouTube and will flag for review videos that incorporate or remix the copyright holder's content.[162] YouTube still adheres to the notice-and-takedown requirements,[163] but Content ID more effectively deters infringement because it can monitor every single video. However, there are two problems with Content ID: First, YouTube invested in its development, meaning that YouTube has borne the largest burden in deterring infringement with Content ID; and second, because YouTube developed it, YouTube alone uses it.

Safe harbor rulemaking would address both of these problems. Content ID is not wholly novel software: Audible Magic is nonproprietary software written for the same purpose.[164] Unfortunately, development of Audible Magic has lagged behind Content ID because liabilities under the DMCA undercut incentives to develop Audible Magic.[165] The content industry had no incentive to invest in Audible Magic because online video-sharing companies have no obligation to

---

[160] In its earliest iterations, Content ID was called Video ID. That the plaintiffs are not litigating over YouTube's behavior after Content ID's implementation shows the content industry's appreciation of the software. *See also* Brief for the Defendants-Appellees at 9, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012) (No. 10-3270) ("YouTube offered Content ID to Viacom as soon as it launched, and Viacom signed an agreement to start using the technology in February 2008.").

[161] *Content ID*, YOUTUBE, http://www.youtube.com/t/contentid (last visited Aug. 8, 2012). YouTube describes Content ID as "designed for exclusive rights holders whose content is frequently uploaded to YouTube by the user community." *Id.*

[162] *Id.*

[163] *See Copyright Infringement Notification*, YOUTUBE, http://www.youtube.com/t/dmca_policy (last visited Aug. 8, 2012) (offering instructions on filing a proper takedown letter).

[164] *Solutions for Content Owners*, AUDIBLE MAGIC, http://audiblemagic.com/solutions-contentowners.php (last visited Aug. 8, 2012). Audible Magic boasts eleven million "fingerprints" of copyrighted audiovisual content, "represent[ing] over 900,000 hours of copyrighted songs, movies, television shows, and other video content." *Id.*

[165] YouTube first began using Audible Magic in early 2007 but started developing Content ID out of frustration with Audible Magic's limitations. *See* Brief for the Defendants-Appellees at 8, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012) (No. 10-3270) (noting that "none of the plaintiffs were using [Audible Magic] to protect their copyrights before they filed [the] lawsuit").

install it. Instead, major content companies have invested in losing lawsuits.[166] Under a safe harbor rulemaking regime, the content industry would have greater incentive to invest in the development of technology like Audible Magic—or other safe harbor startups—because, once developed, they could petition for rulemaking that conditions safe harbor protection of video-sharing sites on the use of such technology. Under this model, the content industry would bear more of the upfront costs of deterring infringement,[167] and the resultant technology would be usable by more than one service provider.[168]

C. Private Cloud Services and the Public Benefit of Safe Harbor Rulemaking

The private cloud services problem highlights the core policy problems of copyright online. Overly protected copyright entitlements undermine technological innovation,[169] whereas underprotected copyright entitlements undermine incentives for creators to produce

---

[166] Content companies lost in the Ninth Circuit against video-sharing site Veoh, UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1050 (9th Cir. 2011), and lost in the Southern District of New York against YouTube, Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 529 (S.D.N.Y. 2010), *aff'd in part, vacated in part, rev'd in part*, 676 F.3d 19 (2d Cir. 2012). Although the Second Circuit reversed the district court summary judgment, it is not clear that this is a winning result for Viacom. *See supra* notes 150–52 and accompanying text (discussing the Second Circuit's *YouTube* decision).

[167] This is not meant to suggest that service providers would bear no costs in implementing a technology like Audible Magic—they will pay licensing (or purchasing) fees and will bear the costs of integrating Audible Magic into their own system. But these costs are substantially less than the upfront costs of developing the technology, which are costs that a rulemaking regime would encourage content owners to subsidize. The balance of these costs better mirrors those of notice and takedown.

[168] Extremely wealthy technology companies like YouTube (which is owned by Google) should still be able to develop proprietary deterrent measures. Such companies' expertise with their own technology suggests they will often be able to develop better versions of deterrent measures. A safe harbor rulemaking regime may promote this by establishing two different thresholds of proof for approval of deterrent measures: Novel measures must pass a higher burden of proof to be issued in rulings, but service providers may be eligible for letter rulings approving proprietary versions of previously approved measures so long as the proprietary versions are at least as effective as the previously approved measures. *See supra* notes 139–42 and accompanying text (discussing necessary considerations in the approval of new measures).

YouTube benefits from Content ID not only because it promotes a cooperative relationship with the content industry and lessens its risk of liability but also because it increases the reach of YouTube's advertising. Copyright holders can elect to permit infringing user-uploaded videos to remain online with the addition of ads, the profits of which are split by the copyright holder and YouTube. *See Content ID*, *supra* note 161 (advertising Content ID as a way to "[m]ake [m]oney").

[169] This is the problem that motivated the DMCA's passage in the first place. *See supra* note 7 (describing the *Netcom* case that precipitated the DMCA's passage).

and release new copyrightable work.[170] These concerns pit the interests of copyright holders against those of the Internet industry. The interests of the public are implicated secondarily in public access to new technologies and new cultural goods.

The DMCA appears clearly to promote both technological innovation and copyright holders' interest in their exclusive entitlements. But the DMCA's policy of promoting copyright protection can be read more broadly to mean promoting the underlying bargain of copyright—the balance of the creator's just reward and economic recoupment against the public's interest in entertainment, intellectual advancement, and an autonomous right of free expression. The public's interest is not just in the creation of *new* cultural and knowledge goods, but also in access to—and use of—*existing* cultural and knowledge goods. Thus, the general grant of exclusive rights under copyright is qualified by numerous exceptions promoting this public interest, such as fair use[171] and first sale.[172]

Liability rules under the DMCA affect this public interest as much as they affect the development of new works and new technologies. Unclear liability rules may lead content companies to self-help bargaining with the largest technology companies.[173] Although it is

---

[170] *See, e.g.*, William M. Landes & Richard A. Posner, *An Economic Analysis of Copyright Law*, 18 J. LEG. STUD. 325, 326 (1989) (describing copyright as an economic incentive for creation).

[171] Fair use is too amorphous and complex a doctrine to explain in a footnote. For further information, see *supra* note 25 and accompanying text.

[172] The first sale doctrine is codified at 17 U.S.C. § 109 (2006). The first sale doctrine allows one to resell or give away a previously purchased copy of a book (or CD, DVD, etc.) without that resale or gift violating the copyright owner's exclusive right of distribution. § 109(a). Similarly, the first sale doctrine allows one to publicly display that copy without violating the owner's public display right. § 109(c). More broadly, first sale is an example of copyright exhaustion, a concept that limits the extent of the copyright holder's monopoly to achieve an optimal balance of copyright's policy goals. *See generally* Aaron Perzanowski & Jason Schultz, *Digital Exhaustion*, 58 UCLA L. REV. 889, 908–25 (2011) (describing exhaustion).

[173] The DMCA purports to encourage copyright holders to put their content online, but given the inefficiencies of notice and takedown, *see supra* notes 155–57 and accompanying text, content owners have shown understandable reluctance to offer their content online and risk losing further control over its distribution. Bereft of rights enforcement alternatives to litigation or the notice-and-takedown regime, the content industry has struggled to establish a positive working relationship with major technology players, fueling the sometimes anti-digital stance of the content industry—which in turn may have contributed to widely espoused user viewpoints that discount the legitimacy of the content industry's interests. But this may be changing. In 1998, the online industry was small and lacked stable, dominant players, whereas in the last five years, the Internet accounted for twenty-one percent of GDP growth in mature economies. JAMES MANYIKA & CHARLES ROXBURGH, MCKINSEY GLOBAL INST., THE GREAT TRANSFORMER: THE IMPACT OF THE INTERNET ON ECONOMIC GROWTH AND PROSPERITY 1 (2011), *available at* http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/The_great_

hard to predict how such self-help would unfold, neither the interests of the public nor the interests of small players or small technology startups are likely to be represented.

A current example of this may be Apple's version of the MP3tunes service. Before its launch, newspapers rumored that Apple was paying the four largest music companies up to $150 million in licensing royalties.[174] The remarkable feature of Apple's service is that consumers may never need to upload their songs into their music locker;[175] instead, Apple scans a user's computer to identify song files and then grants the user streaming and downloading access to Apple's own copies of those songs.[176] Even users with poor-quality songs pirated from peer-to-peer and torrent networks can replace those versions with high-quality copies from Apple without paying a per-song fee.[177]

Music companies receive an obvious benefit in the licensing royalties,[178] but they also benefit from Apple's platform lock-in. Because

---

transformer. By February 2012, Apple was the most valuable public company in the world. James B. Stewart, *Confronting a Law of Limits*, N.Y. TIMES, Feb. 25, 2012, at B1. And as the online industry has grown, the content industry has shown increased willingness to bargain with the most salient companies—consider, for example, Apple's role in legitimizing digital music through iTunes. *See* John Markoff, *Apple Sells 70 Million Songs in First Year of ITunes* [sic] *Service*, N.Y. TIMES, Apr. 29, 2004, http://www.nytimes.com/2004/04/29/business/technology-apple-sells-70-million-songs-in-first-year-of-itunes-service.html (describing the "breakthrough" success of iTunes's first year).

174 Claire Atkinson, *Apple Pays Music Bigs $100M+*, N.Y. POST, June 3, 2011, 12:10 AM), http://www.nypost.com/p/news/business/apple_pays_music_bigs_OcxlGqT1E0P5P9vzosxtyK. Later reports also suggested that the music companies would continue to receive royalties from Apple, receiving a share of subscription fees based on the frequency with which each song is streamed through Apple's service. *See* Ganz, *supra* note 99 ("For record labels and musicians, there's another upside: because Apple will be able to track how many times each song in iTunes is streamed on a user's device, musicians and songwriters could be paid royalties.").

175 Apple touts this as a significant user benefit: Users don't waste time uploading huge music libraries—"a process that could take hours or days . . . ." Ganz, *supra* note 99.

176 *iCloud Features*, APPLE, http://www.apple.com/icloud/features/ (last visited Aug. 8, 2012).

177 E.B. Boyd, *iTunes Match Not Laundering Pirated Music, It's Driving a Subscription Future*, FAST COMPANY (June 8, 2011), *available at* http://www.fastcompany.com/1758202/music-executives-itunes-match-is-an-important-stepping-stone-toward-our-collective-subscript ("[I]t appears that Apple is not going to distinguish between authorized and unauthorized tunes . . . ."). The only cost is an annual $24.99 subscription fee. *iCloud Features*, *supra* note 176.

178 They do not receive such royalties from competing services like MP3tunes, but perhaps more notably, royalties under Apple's program allow them to nominally monetize pirated music. *See* Boyd, *supra* note 177 ("[T]he music industry might finally earn some money on illegally downloaded tunes that were previously pure loss."). Unsurprisingly, the music companies want to see Google and Amazon adopt licensing deals for their cloud services as well. *See* Jacqui Cheng, *Music Industry Will Force Licenses on Amazon Cloud Play—or Else*, WIRED: EPICENTER (Apr. 2, 2011, 9:30 AM), http://www.wired.com/

Apple's cloud services function on Apple devices, Apple can exert greater control over who logs into a private cloud account to download songs than the control offered by independent services like MP3tunes or Dropbox—meaning that Apple can better limit the use of its service for infringing activities. Apple similarly benefits from the subscription fees as well as from the services and upgrade fees paid by users locked into its platform.

However, ordinary consumers do not benefit. Small competitors lack Apple's bargaining power[179] and therefore cannot imitate many features of Apple's service without violating copyright law.[180] Most importantly, because of unclear liability under the DMCA, they do not know what they can and cannot offer consumers as alternatives. As a result, users will find diminished innovation in private cloud services.

Further, Apple's service may be the harbinger of a "subscription future."[181] Subscription-only services would prevent consumers from using cloud services to infringe copyrights but would also strip consumers of their property interests in purchased content. For example, subscription models threaten to undermine or entirely erode the first sale doctrine:[182] Because users will not own digital copies of music, movies, and books that they purchase, users will have no legal right to sell or gift those copies to others—or to otherwise use those copies as they wish. The reduced-price market would evaporate,[183] potentially

epicenter/2011/04/music-industry-cloud-player/all/1 (noting the music industry's incentive to force Google and Amazon to adopt licensing).

179 Similarly, the bargains reached between major technology companies and major content companies exclude small, independent content companies. Independent labels are less enthusiastic about Apple's service, but face a Hobson's choice: Accept Apple's terms or be left out. *See, e.g.*, Chris Foresman, *Why iTunes Match Has Indie Soul Label Singing the Blues*, ARS TECHNICA (June 16, 2011, 11:47 AM), http://arstechnica.com/apple/news/2011/06/why-itunes-match-has-indie-soul-label-singing-the-blues.ars.

180 For example, without similar licensing agreements, MP3tunes could not offer its own copies of songs for download the way Apple does because it would be knowingly infringing copyright with each download and therefore would be ineligible for DMCA safe harbor. *See supra* Part I.A (outlining the requirements for the DMCA safe harbor).

181 Boyd, *supra* note 177 ("[iTunes Match] will be useful for where we're all headed: subscription services. In five or ten years, . . . consumers won't be buying individual tracks and albums."). Apple's iCloud is not the only evidence of a trend toward subscriptions. For example, the rejected Google Books Settlement included a program whereby consumers purchased licenses, rather than copies, of digital books. Amended Settlement Agreement § 4.7(c), Authors Guild v. Google, Inc., 770 F. Supp. 2d 666 (2d Cir. 2011) (No. 05 CV 8136-DC).

182 For a brief introduction to the first sale doctrine, see *supra* note 172.

183 One online service, ReDigi, purports to offer resale of digital files. The service scrubs copies of a file from a user's computer on sale. *See Learn More About ReDigi*, REDIGI, https://www.redigi.com/#!/learn (last visited Aug. 8, 2012). However, it is unclear how ReDigi would prevent a user from merely reselling a song and letting ReDigi delete the

diminishing the access of lower-income consumers to knowledge goods.[184]

Thus, in the context of private cloud services, the content industry faces three options. First, it can utilize notice and takedown when possible but otherwise ignore private cloud services.[185] This solution is unsatisfactory: Rights holders would be relinquishing those rights simply because no good remedy exists. Second, copyright holders can litigate, which is costly for both the technology and content industries, undermining innovation in both industries. Finally, the content industry can bargain directly with private cloud services, but this option threatens to undermine both technological innovation and the public-benefit limitations on copyright.

The safe harbor rulemaking revisions suggested in Subpart II.A better address the private cloud services problem because the revisions first make clear that private cloud services receive DMCA protection and, second, implement a mechanism through which infringement can better be deterred. Still, the precise nature of anti-infringement measures targeting private cloud services is impossible to predict. A measure may, for example, utilize file-fingerprinting technology akin to Content ID and Audible Magic to limit permissible files in "shared" folders on services like Dropbox. Or an anti-infringement measure for private cloud services may never develop—perhaps because no effective measure exists or perhaps because content owners would prefer to focus their resources combating other instances of infringement. Such an outcome does not undermine the

song from the user's computer, then recopying the song back onto the computer from an MP3 player, Dropbox, or some other service or device. ReDigi is currently headed to trial. *See* David Kravets, *Judge Refuses To Shut Down Online Market for Used MP3s*, WIRED: THREAT LEVEL (Feb. 7, 2012, 2:34 PM), http://www.wired.com/threatlevel/2012/02/pre-owned-music-lawsuit-2/ (quoting the judge's statement from the bench that the "liklihood [sic] of success on the merits is something that plaintiffs have demonstrated," suggesting that denial of summary judgment rested on other grounds and that ReDigi's chances at trial currently do not look promising). *But see* Perzanowski & Schultz, *supra* note 172, at 935–39 (arguing that exhaustion should permit services like ReDigi).

184 Theoretically, the first sale doctrine promotes the constitutional goal of copyright to promote knowledge because the reduced-price market it enables expands the audience of knowledge goods. *See* Perzanowski & Schultz, *supra* note 172, at 894–95 (discussing the role of first sale in "improv[ing] both the affordability and availability of copyrighted works").

185 Although turning a blind eye would permit infringement, this is not an unrealistic possibility. Given the volume of infringement online, copyright holders must judiciously pick their battles. They may not find infringement in private cloud services to be egregious enough to require new or aggressive solutions. *See supra* notes 100–03 and accompanying text (comparing the VHS and the Napster problems of infringement online). They may also fear that litigation over the DMCA and private cloud services could result in unfavorable precedent.

value of safe harbor rulemaking. The goal and chief benefit of safe harbor rulemaking is not to provide an immediate solution to the private cloud services problem but to provide a flexible mechanism that leads to the development of solutions as new technologies arise. Safe harbor rulemaking reaffirms copyright holders' ability to enforce their individual rights without threatening legitimate innovation. And clear upfront liability rules protect the public's interest.

Conclusion

If the DMCA was the law that "saved the Web,"[186] then it was likely a temporary grace. The DMCA's regulatory-like specificity and complexity will become increasingly dated in the face of innovation online. Extending safe harbor immunity to private cloud services already contravenes the DMCA's goal of combating infringement because the DMCA's one cooperative anti-infringement mechanism—notice and takedown—has no effect on private cloud services. Revising the DMCA to allow safe harbor rulemaking would inject flexibility into its regulatory scheme and create avenues for copyright holders to develop new cooperative anti-infringement measures specifically adapted to previously unforeseen technologies, like private cloud services. Properly balanced, safe harbor rulemaking can better protect copyright holders' interests without threatening technological innovation or public access to knowledge goods.

---

[186] Kravets, *supra* note 8.