
WHO'S ON THE HOOK FOR DIGITAL
PIRACY? AN ANALYSIS OF PROPOSED
CHANGES TO THE DIGITAL
MILLENNIUM COPYRIGHT ACT AND
SECONDARY COPYRIGHT
INFRINGEMENT CLAIMS

ERIKA PANG

TABLE OF CONTENTS

INTRODUCTION.....	1274
I. THE DIGITAL MILLENNIUM COPYRIGHT ACT.....	1277
A. INTRODUCTION TO UNITED STATES COPYRIGHT LAW AND THE DMCA	1277
B. POLICY GOALS UNDERLYING THE DIGITAL MILLENNIUM COPYRIGHT ACT.....	1280
2. Eligibility Requirements for All Safe Harbors Under 17 U.S.C. § 512(i)	1282
3. Specific Requirements for Safe Harbor Eligibility Under Section 512(a) and (c)	1283
II. PROPOSALS TO REFORM THE DIGITAL MILLENNIUM COPYRIGHT ACT	1286
A. THERE ARE TWO COMPETING POLICIES CONCERNING THE EFFICACY OF THE DIGITAL MILLENNIUM COPYRIGHT ACT	1286
B. THE DUTY TO MONITOR AND THE ADOPTION OF A NOTICE AND STAY-DOWN SYSTEM ARE POTENTIAL AREAS OF REFORM	1292
1. The Relationship Between the Knowledge Requirement and the Lack of Imposition of Duty to Monitor Requires Clarification	1292

2. Updating the Digital Millennium Copyright Act with a Notice and Stay-Down System.....	1293
III. INTERNET SERVICE PROVIDERS AND SECONDARY COPYRIGHT INFRINGEMENT LIABILITY	1294
A. HISTORY OF SECONDARY LIABILITY FOR COPYRIGHT INFRINGEMENT.....	1294
1. Contributory Liability Test	1295
2. Vicarious Liability Test	1297
B. CURRENT STANDARDS FOR SECONDARY LIABILITY ARE LESS CLEAR WHEN APPLIED TO PASSIVE INTERNET SERVICE PROVIDERS	1298
C. “MERE CONDUIT” INTERNET SERVICE PROVIDERS CURRENTLY FACE LITIGATION CONCERNING SECONDARY LIABILITY CLAIMS	1299
IV. CLARIFIED SAFE HARBOR PROTECTION AND INTERNET SERVICE PROVIDER INSULATION FROM LIABILITY ARE NECESSARY	1301
A. ANALYSIS OF PROPOSED AMENDMENTS TO THE DMCA.....	1301
B. A NARROW READING OF VICARIOUS LIABILITY DOCTRINE APPLIED TO ISPs	1304
CONCLUSION	1305

INTRODUCTION

*FBI Anti-Piracy Warning: The unauthorized reproduction or distribution of a copyrighted work is illegal. Criminal copyright infringement, including infringement without monetary gain, is investigated by the FBI and is punishable by up to five years in federal prison and a fine of \$250,000.*¹

Chances are that many Americans have seen the warning above at some point in their lives, whether they saw the words stamped on the back of a music album sleeve or displayed on a screen before viewing a film.² Still, despite the threat of severe liability, chances are that many of these

1. *FBI Anti-Piracy Warning Seal*, FED. BUREAU OF INVESTIGATION, <https://www.fbi.gov/investigate/white-collar-crime/piracy-ip-theft/fbi-anti-piracy-warning-seal> [<https://perma.cc/6HEN-PT3G>].

2. *See id.* All U.S. copyright holders are authorized by 41 C.F.R. § 128-1.5009 to use the FBI’s Anti-Piracy Warning (“APW”) Seal, the purpose of which is to deter infringement of U.S. intellectual property laws by educating the public of these laws’ existence and notifying citizens of the FBI’s authority to enforce these laws. *Id.*

individuals will nevertheless engage in illegal pirating activity.³

Prior to the rise of the internet, individuals who made illegal copies of copyright-protected works like movies and music recordings were necessarily limited by the technology available to make such copies.⁴ Magnetic audio and videotape cassettes allowed individuals to record songs played on the radio or movies and television shows to create “bootleg” versions by crude processes which, by nature, hindered one’s ability to reproduce multiple copies of similar quality to the original work.⁵ However, as technology progressed, the opportunities to create illegal copies of copyrighted works, specifically within the newly emerging digital landscape, expanded with ease, and digital piracy grew more and more rampant.⁶ The development of compact discs (“CDs”) and MP3 compression software provided easier avenues to create impermissible copies of digital media, and access to high-speed internet coupled with the rise of peer-to-peer sharing systems streamlined opportunities for fast and simple illegal downloading.⁷ Today, in the current landscape of internet ubiquity, digital piracy has become an all but inevitable obstacle that every copyright owner, be it a large established entity such as a record label or a small independent content creator, has come to anticipate.⁸

The issue of digital piracy has not gone unaddressed by Congress, as evidenced by the promulgation of the Digital Millennium Copyright Act (“DMCA”) in 1998.⁹ One goal of the DMCA was to address the growing rates of digital piracy in the 1990s by providing copyright owners additional causes of action against copyright infringers, particularly infringers that impermissibly circumvented technological tools used by rights-owners to

3. Maria Petrescu, John T. Gironde & Pradeep K. Korgaonkar, *Online Piracy in the Context of Routine Activities and Subjective Norms*, 34 J. MKTG. MGMT. 314, 324–25 (2018). Studies have shown that although some consumers may view digital piracy as an infringement of another’s intellectual property rights, this did not impact their moral perceptions of the act of infringement. *Id.* Digital piracy may be regarded as a “soft crime,” as one study noted that consumers who state they would not steal a CD from a store would still consider illegally downloading the contents of the CD online, due to a lowered risk of getting caught. *Id.* at 325.

4. Thomas J. Holt & Steven Caldwell Brown, *Contextualising Digital Privacy*, in DIGITAL PIRACY: A GLOBAL, MULTIDISCIPLINARY ACCOUNT 3, 4 (Steven Caldwell Brown & Thomas J. Holt eds., 2018).

5. *See id.*

6. *See id.*

7. *See id.*

8. *See id.* The authors note that “it is thought that millions of people engage in digital piracy every day. The true scope of piracy is, however, difficult to document as clear statistics are difficult to obtain.” *Id.* at 5. One report by Music Watch estimated 57 million Americans pirated digital copies of music in 2016; another report by Nera estimated the revenue loss for the global movie industry to be between \$40 billion and \$97.1 billion per year. Damjan Jugović Spajić, *Piracy Statistics for 2021*, DATAPROT (March 19, 2021), <https://dataprot.net/statistics/piracy-statistics/> [<https://perma.cc/5CMV-BH8N>].

9. Digital Millennium Copyright Act of 1998, 17 U.S.C. §§ 512, 1201–02.

protect their works.¹⁰ However, the drafters of the DMCA were also careful to remain consistent with the main underpinnings of copyright law, which are to maintain a balance between protecting copyright owners' works and facilitate the constitutional charge to "promote the Progress of Science and useful Arts."¹¹ Within the context of the emerging digital age, Congress applied this balance by seeking to (1) instill confidence in rightsholders that copyright protections would remain effective in a digital landscape and (2) provide assurances to new, growing online service providers ("OSPs") that their unprecedented business models would not be decimated by imputing liability to the providers for the infringing conduct of their users.¹² Thus, Title I of the DMCA laid out "anti-circumvention provisions" that prohibit circumvention of technological measures, such as password keys and encryption codes, used to protect copyrighted works.¹³ Title II of the DMCA mitigated liability for internet service providers ("ISPs")¹⁴ by granting "safe harbor" protections to ISPs that comply with statutory requirements—these safe harbors largely aimed to incentivize ISPs to promptly respond to reports of infringing content.¹⁵

Since its enactment, the DMCA has received criticism that its measures are outdated and ill-equipped to address the ongoing digital piracy problems that continue today.¹⁶ The internet is undoubtedly a different landscape from what it was at the time the DMCA was promulgated more than two decades ago.¹⁷ With current considerations to amend the DMCA in light of the areas of growth that were unimagined at the time the DMCA was written,¹⁸ coupled with recent litigation seeking to hold ISPs secondarily liable for infringing conduct of their subscribers,¹⁹ the path to reducing digital piracy

10. See Holt & Caldwell Brown, *supra* note 4, at 189; CYBERLAW: INTELLECTUAL PROPERTY IN THE DIGITAL MILLENNIUM § 1.02, Lexis [hereinafter CYBERLAW § 1.02] (database updated Oct. 2020).

11. U.S. CONST. art. I, § 8, cl. 8.

12. See BILL D. HERMAN, *THE FIGHT OVER DIGITAL RIGHTS: THE POLITICS OF COPYRIGHT AND TECHNOLOGY* 45, 48–49 (2013).

13. CYBERLAW § 1.02, *supra* note 10.

14. For the purposes of this Note, the term "ISP" will refer to service providers that merely provide internet access to their subscribers (for example, Charter Spectrum, AT&T, and Frontier). The term "OSP" will refer to all other online service providers that provide services such as user material hosting or system caching (for example, YouTube, Facebook, and Google).

15. CYBERLAW § 1.02, *supra* note 10.

16. See U.S. COPYRIGHT OFF., SECTION 512 OF TITLE 17: A REPORT OF THE REGISTER OF COPYRIGHTS 27–28 (2020) [hereinafter REPORT OF THE REGISTER OF COPYRIGHTS], <https://www.copyright.gov/policy/section512/section-512-full-report.pdf> [<https://perma.cc/R8Z9-JQME>].

17. See *id.*

18. See *id.* at 10.

19. Compare *UMG Recordings, Inc. v. Bright House Networks, LLC*, No. 8:19-CV-710, 2020 U.S. Dist. LEXIS 122774, at *5 (M.D. Fla. July 8, 2020) (declining to hold defendant ISP vicariously liable for user infringement because ISPs do not receive a *direct* financial benefit from ongoing infringement), with *Warner Recs. Inc. v. Charter Commc'ns, Inc.*, 454 F. Supp. 3d 1069, 1079 (D. Colo. Oct. 21, 2019) (holding that defendant ISP may be vicariously liable for infringement because the ISP

is still paved with uncertainty.

Following a discussion of ongoing proposed changes to the DMCA and developing litigation concerning the potential for vicarious liability claims against ISPs, this Note will ultimately argue that the current DMCA safe harbor provisions require updated eligibility requirements for ISPs, but the availability of vicarious liability claims against “mere conduit” ISPs overreaches the scope of protection afforded to copyright owners. Part I will provide a brief history of the DMCA, including a discussion of the safe harbor provisions and the requirements therein. Part II will incorporate current discussions regarding the need for DMCA reform, address the competing policies at play, and note potential areas of reform. Part III will discuss the origins of secondary copyright infringement liability caselaw, including recent cases that have considered extending vicarious liability claims to ISPs that act as “mere conduits” to provide internet to their users. Part IV will propose clarifications in the DMCA safe harbor protection most needed in the current digital landscape while arguing that ISPs must still be properly insulated from open floodgates of liability. This Note will conclude that the DMCA should be revised to alleviate rightsholders’ burden of monitoring incidents of copyright infringement, but the DMCA should still insulate “mere conduit” ISPs from vicarious liability claims.

I. THE DIGITAL MILLENNIUM COPYRIGHT ACT

A. INTRODUCTION TO UNITED STATES COPYRIGHT LAW AND THE DMCA

The enactment of the DMCA constituted a significant amendment to the Copyright Act of 1976.²⁰ Under the 1976 Act, copyright protection is afforded “in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated.”²¹ Thus, materials including literary works, musical works, and motion pictures constitute “works of authorship” that enjoy federal copyright protection once they have been written, recorded, or filmed.²² An author is defined as “the creator of the original expression in a work,” and it is presumed that the author is the owner of the copyright unless the author has given written authorization to

plausibly receives a financial benefit from infringing users “motivated” to use the ISP’s service due to the ISP’s lax approach to curbing infringement).

20. See HERMAN, *supra* note 12, at 37 (“The Digital Millennium Copyright Act . . . arguably represents the most dramatic change in the history of U.S. copyright law.” (quoting TARLETON GILLESPIE, *WIRED SHUT: COPYRIGHT AND THE SHAPE OF DIGITAL CULTURE* 177 (2009))).

21. 17 U.S.C. § 102.

22. See *id.*; MARY LAFRANCE, *COPYRIGHT LAW IN A NUTSHELL* 2 (3rd ed. 2017).

pass the copyright to another individual or entity.²³ Though copyright protection attaches regardless of whether a copyright notice is obtained²⁴ or registration is completed with the United States Copyright Office (the “Copyright Office”),²⁵ owners must typically register their copyright if they seek to enforce their exclusive rights and hold infringers liable.²⁶ Copyright owners are granted the exclusive right to do and authorize the following: (1) reproduce copies of the copyrighted work; (2) create derivative works based on the copyright; (3) distribute copies by sale or other transfer of ownership; (4) perform the copyrighted work publicly; (5) display the work publicly; and (6) perform the work publicly via digital audio transmission.²⁷

The Copyright Act of 1976 was largely geared toward clarifying the contours of U.S. copyright law given the then-novel advent of technology such as photocopy, videotape, and cable television. Similarly, the DMCA served to update existing copyright law to address concerns regarding how copyright law would continue to protect works in the developing digital landscape and whether new, online third-party intermediaries may be held liable for the infringing conduct of individuals who used their services.²⁸ Title I of the DMCA prohibits the circumvention of “a technological measure that effectively controls access to a work,”²⁹ with circumvention involving “deactivating or bypassing a technological safeguard which restricts unauthorized access to the work in question.”³⁰ Notably, the six protected activities within the Copyright Act provide copyright owners with the right to control the *use* of their copyrighted works, but the Copyright Act does not control *access* to these works.³¹ The DMCA remains consistent with this use-access distinction.³² Though the DMCA amended the Copyright Act by

23. *Definitions*, U.S. COPYRIGHT OFF., <https://www.copyright.gov/help/faq-definitions.html> [<https://perma.cc/xB5F-4LKZ>].

24. Effective March 1, 1989, notice is not an essential component to qualifying for copyright protection. LAFRANCE, *supra* note 22, at 106. Notice serves as a statement placed on copies of a copyrighted work indicating that a copyright owner has claimed ownership of the work. *Copyright Notice*, U.S. COPYRIGHT OFF., <https://www.copyright.gov/circs/circ03.pdf> [<https://perma.cc/6E94-F6VT>]. Notice consists of the copyright symbol (“©”) or the word “copyright,” the year of first publication of the work, and the copyright owner’s name. *Id.*

25. Registration generally involves submission of a registration form and filing fee, as well as the deposit of a copy of the work to the Register of Copyrights. LAFRANCE, *supra* note 22, at 120.

26. *Id.* at 418.

27. 17 U.S.C. § 106.

28. HECTOR POSTIGO, *THE DIGITAL RIGHTS MOVEMENT: THE ROLE OF TECHNOLOGY IN SUBVERTING DIGITAL COPYRIGHT* 19 (2012).

29. 17 U.S.C. § 1201.

30. 1 LAW OF THE INTERNET § 5.03, Lexis (database updated Dec. 2021).

31. *See* CYBERLAW: INTELLECTUAL PROPERTY IN THE DIGITAL MILLENNIUM § 3.02, at 2, Lexis (database updated Oct. 2021).

32. *See* INTELLECTUAL PROPERTY AND COMPUTER CRIMES § 3.02, Lexis (database updated Aug. 2018).

equipping copyright owners with additional “causes of action for liability” through the anti-circumvention provisions, the DMCA did not create new property rights to be afforded to copyright owners.³³

Title II of the DMCA, codified in 17 U.S.C. § 512 (“section 512”), limited the liability of OSPs for infringement “in those instances in which the service provider is unaware of the infringing materials or otherwise acts promptly to remove the infringing material upon notice.”³⁴

Prior to Title II of the DMCA, courts were beginning to develop a body of caselaw that addressed whether OSPs could be held liable for copyright infringement carried out by the OSPs’ users.³⁵ In *Playboy Enterprises, Inc. v. Frena*, a computer bulletin board operator was found directly liable for copyright infringement for posting the plaintiff’s copyrighted photos without authorization.³⁶ Although the operator did not himself post the infringing material and removed the material once he was provided notice of the infringement, the court still held that “[i]ntent to infringe is not needed to find copyright infringement [T]hus even an innocent infringer is liable for infringement.”³⁷ Contrary to *Frena*, one California district court declined to hold an ISP directly liable for its users’ infringement of copyrighted materials in *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*³⁸ The *Netcom* court instead held that

[w]here the infringing subscriber is clearly directly liable for the same act, it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet.³⁹

The existence of such conflicting decisions in the developing caselaw concerning OSPs’ potential liability for infringing users created uncertainty regarding the scope of liability that OSPs should be held to, with many OSPs fearing that they may be “sued out of existence for involvement in purportedly aiding copyright infringement.”⁴⁰ For the purposes of this Note, discussion surrounding the DMCA will primarily focus on section 512 and the legal framework it introduced with regards to OSPs’ infringement liability limitations.

33. *Id.*

34. *Id.*

35. REPORT OF THE REGISTER OF COPYRIGHTS, *supra* note 16, at 14–15.

36. *Playboy Enters., Inc. v. Frena*, 839 F. Supp. 1552, 1559 (M.D. Fla. 1993).

37. *Id.*

38. *Religious Tech. Ctr. v. Netcom On-Line Comme’n Servs., Inc.*, 907 F. Supp. 1361, 1368–70 (N.D. Cal. 1995).

39. *Id.* at 1372.

40. 4 NIMMER ON COPYRIGHT §12B.01(c)(1) (2020), Lexis (database updated Dec. 2021).

B. POLICY GOALS UNDERLYING THE DIGITAL MILLENNIUM COPYRIGHT ACT

With the turn of the century, Congress intended the DMCA to address widespread “massive piracy” problems by “appropriately balanc[ing] the interests of content owners, on-line and other service providers, and information users in a way that will foster the continued development of electronic commerce and the growth of the Internet.”⁴¹ Additionally, the DMCA served as legislation that conformed United States copyright law with obligations to World Intellectual Property Organization (“WIPO”) treaties, which required signatory governing bodies to provide effective legal remedies against the circumvention of “technological measures” used to protect copyrighted works.⁴² While the rise in digital piracy posed a sizable threat to the protections afforded copyright owners, Congress was wary of imposing too much liability on service providers, which could, in turn, stifle the ongoing development and expansion of internet services.⁴³ Congress enacted Title II of the DMCA as the solution to both (1) provide means for rights-owners to combat incidences of infringement found online and (2) stimulate the development of OSPs by clarifying OSPs’ obligations to monitor third-party infringement and providing potential limitations on OSPs’ liability for infringing users.⁴⁴

When drafting the DMCA, Congress was largely concerned with balancing the interests of copyright owners with the interests of a community of “users, scholars, equipment manufacturers, and online service providers.”⁴⁵ Commentary from the House Commerce Committee clearly illustrates the pervasive nature of this balancing act:

The debate on this legislation highlighted two important priorities: promoting the continued growth and development of electronic commerce; and protecting intellectual property rights. These goals are mutually supportive. A thriving electronic marketplace provides new and powerful ways for the creators of intellectual property to make their works available to legitimate consumers in the digital environment. And a plentiful supply of intellectual property—whether in the form of software, music, movies, literature, or other works—drives the demand for a more flexible and efficient electronic marketplace.⁴⁶

41. *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081, 1090 (C.D. Cal. 2008) (quoting H.R. REP. NO. 105-551, pt. 2, at 21 (1998)).

42. INTELLECTUAL PROPERTY AND COMPUTER CRIMES, *supra* note 32, at 24.

43. *Id.*

44. REPORT OF THE REGISTER OF COPYRIGHTS, *supra* note 16, at 19–20.

45. David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 681–82 (2000).

46. H.R. REP. NO. 105-551, pt. 2, at 22–23 (1998).

To achieve this balance, Congress introduced a system in which OSPs could limit their copyright liability, now known as “safe harbors,” so long as the OSP met certain conditions, such as removing infringing material promptly upon receiving notice from a rightsholder.⁴⁷ The system was also intended to benefit rightsholders by incentivizing them to take part in “an expeditious and extra-judicial method” for addressing infringement of their works.⁴⁸

C. SAFE HARBOR PROTECTIONS OF THE DIGITAL MILLENNIUM COPYRIGHT ACT

The DMCA provides four safe harbor protections to limit OSP liability for infringing users’ activity, and each safe harbor is treated separately from one another, although some share common provisions.⁴⁹ The limitations are based on four categories of conduct by a service provider: (1) transitory communications; (2) system caching; (3) storage of information on systems or networks at the direction of users; and (4) information location tools.⁵⁰ Section 512(l) explicitly notes that if an OSP fails to qualify for safe harbor protection, this failure will not “bear adversely” upon the defense used by the OSP in later litigation concerning the OSP’s potential infringement liability.⁵¹ In other words, the safe harbor provisions “do not affect the question of ultimate liability under the various doctrines of direct, vicarious, and contributory liability” that are introduced in common law, but a defendant that comes under safe harbor protection may escape monetary liability and significantly limit the scope of injunctive relief.⁵²

1. Definitions of “Service Provider” Under the Digital Millennium Copyright Act

Section 512(k) delineates the definition of a “service provider” for the purposes of safe harbor availability.⁵³ Subsection (a), which concerns the transitory communications safe harbor, defines a “service provider” as “an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the

47. See REPORT OF THE REGISTER OF COPYRIGHTS, *supra* note 16, at 1.

48. *Id.*

49. See 1 LAW OF THE INTERNET § 5.03, *supra* note 30, at 24.

50. 17 U.S.C. § 512(a)–(d).

51. *Id.* § 512(l).

52. ENTERTAINMENT LAW & LITIGATION § 4.07, at 1, Lexis (database updated 2019) (quoting Perfect 10, Inc. v. Cybernet Ventures, Inc., 2013 F. Supp. 2d 1146, 1174 (C.D. Cal. 2002)).

53. 17 U.S.C. § 512(k).

material as sent or received.”⁵⁴ Subsections (b)–(d), which concern the system caching, information storage, and information location tools safe harbors, define a “service provider” as “a provider of online services or network access, or the operator of facilities therefor.”⁵⁵ The distinction between these two definitions may be best understood by example. The service provider in subsection (a) serves as a “mere conduit” for a user’s activity, such as a company that merely provides and facilitates internet service to its subscribers.⁵⁶ While, on the other hand, the service provider in subsections (b)–(d) includes an expanse of online entities that provide services, such as video-sharing sites like YouTube and Vimeo as well as search engines like Google and Yahoo.⁵⁷

2. Eligibility Requirements for All Safe Harbors Under 17 U.S.C. § 512(i)

There are two overall conditions that a service provider must meet to become eligible for safe harbor protection, common to all four of the safe harbors: (1) the service provider must show it “has adopted and reasonably implemented . . . a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider’s system or network who are repeat infringers,” and (2) the provider must accommodate and refrain from interfering with “standard technical measures” that copyright owners use to uniquely identify or protect their works.⁵⁸

In *Ellison v. Robertson*, the Ninth Circuit found that a triable issue of fact existed with regards to the defendant service provider’s eligibility for safe harbor protection pursuant to the eligibility requirements in section 512(i).⁵⁹ In *Ellison*, several digital files containing the contents of copyrighted books were uploaded to AOL discussion boards.⁶⁰ The author of the books provided written notice to AOL pursuant to DMCA notice requirements, but AOL claimed it never received the notice.⁶¹ Ultimately, the court found that section 512(i)(1)(A) entails three separate requirements for the safe harbor protection: the service provider must (1) adopt a policy that terminates service access for repeat copyright infringers in certain circumstances; 2) inform all users of the service policy; and (3) implement

54. *Id.*

55. *Id.*

56. See REPORT OF THE REGISTER OF COPYRIGHTS, *supra* note 16, at 1 n.1.

57. *Id.*

58. 17 U.S.C. § 512(i).

59. *Ellison v. Robertson*, 357 F.3d 1072, 1090 (9th Cir. 2004).

60. *Id.* at 1074–75.

61. *Id.*

the policy in a reasonable manner.⁶² Since there were facts that suggested AOL had not seen the author's notice of infringement because AOL had failed to implement a system that would have provided AOL to see the email notification, these facts indicated potential ineligibility for safe harbor protection because "AOL allowed notices of potential copyright infringement to fall into a vacuum and to go unheeded," thereby resulting in a policy that was not "reasonably implemented" to address repeat infringers.⁶³

3. Specific Requirements for Safe Harbor Eligibility Under Section 512(a) and (c)

For the purposes of this Note, analysis of the four safe harbor provisions will focus primarily on the third provision: the storage of information on systems or networks at the direction of the service provider's users.

The storage of information safe harbor requires four conditions that a service provider must meet to avoid liability: (1) the service provider must not have "actual knowledge" of the infringing material or activity *or* the provider must not be "aware of facts or circumstances from which infringing activity is apparent;" (2) if the service provider has the right and ability to control the infringing activity of its users, the provider must not receive a "direct financial benefit" from the activity; (3) the service provider must promptly remove or disable access to any infringing activity upon receiving notice; and 4) the provider must publicly identify an agent that is designated to receive notices of claimed infringement.⁶⁴

The storage of information safe harbor has been subject to frequent litigation, particularly with regards to the first provision, which removes protection when a provider becomes "aware of facts or circumstances that make the infringing activity apparent."⁶⁵ This "awareness," otherwise known as "red flag" knowledge, is distinct from *actual* knowledge.⁶⁶ Actual knowledge involves "knowledge of specific and identifiable infringements" of particular individual items, which may be established through the receipt of a takedown notice, but it may also be established by showing that the OSP is otherwise informed of the infringement through means other than a

62. *Id.* at 1090.

63. *Id.* at 1080.

64. 17 U.S.C. §512(c); LAFRANCE, *supra* note 22 at 418; CYBERLAW: INTELLECTUAL PROPERTY IN THE DIGITAL MILLENNIUM § 2.05, Lexis (database updated Oct. 2020).

65. 17 U.S.C. § 512(c)(1)(A)(i)-(ii).

66. See CONG. RSCH. SERV., R43436, SAFE HARBOR FOR ONLINE SERVICE PROVIDERS UNDER SECTION 512(C) OF THE DIGITAL MILLENNIUM COPYRIGHT ACT (2014) [hereinafter CRS REPORT], <https://crsreports.congress.gov/product/pdf/R/R43436/3> [<https://perma.cc/K6A2-N3PT>].

takedown notice.⁶⁷ In *Viacom International, Inc. v. YouTube, Inc.*, the court suggested that the distinction between actual and red flag knowledge may be best understood as the difference between a subjective and objective test: “the actual knowledge provision turns on whether the provider actually or ‘subjectively’ knew of specific infringement, while the 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.”⁶⁸

In *Columbia Pictures Industries v. Fung*, an operator of a peer-to-peer software system was found to have red flag knowledge of infringement for several reasons: (1) the defendant had used the software system himself to download copyrighted material; (2) a majority of files that were downloaded through the program were infringed materials; and (3) the website associated with the defendant frequently promoted lists of content, most of which were infringed copyright works.⁶⁹ Notably, in *Viacom International Inc. v. YouTube, Inc.*, Viacom argued YouTube should be held liable for the infringing conduct of its users because YouTube had generalized knowledge that the infringement was occurring on its platform.⁷⁰ However, the *Viacom* district court held that

[m]ere knowledge of prevalence of such activity in general is not enough. . . . To let knowledge of a generalized practice of infringement in the industry, or of a proclivity of users to post infringing materials, impose responsibility on service providers to discover which of their users’ postings infringe a copyright would contravene the structure and operation of the DMCA.⁷¹

Despite the condition that OSPs may not ignore such red flag knowledge if they would like to seek protection under the safe harbor, section 512(m) clearly states that OSPs are under no duty to monitor their service or “affirmatively seek[] facts indicating infringing activity.”⁷²

D. NOTICE AND TAKEDOWN PROCEDURE UNDER THE DIGITAL MILLENNIUM COPYRIGHT ACT

One of the eligibility requirements for section 512(c) safe harbor protection is that the OSP responds “expeditiously” to remove infringing

67. REPORT OF THE REGISTER OF COPYRIGHTS, *supra* note 16, at 114.

68. *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 31 (2d Cir. 2012).

69. *Columbia Pictures Indus., Inc. v. Fung*, 710 F.3d 1020, 1043–44 (9th Cir. 2013).

70. *See Viacom Int’l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514, 523 (S.D.N.Y. 2010).

71. *Id.*

72. 17 U.S.C. § 512(m).

content for which it has received notice.⁷³ Credited as the “backbone” of the section 512 safe harbor provisions, the notice-and-takedown procedure can be viewed as creating a collaborative effort between rightsholders and OSPs to combat incidences of digital piracy.⁷⁴ On one hand, since the DMCA will not hold an OSP liable for infringing material it was not aware of, rightsholders are incentivized to notify OSPs of infringing content so that the OSP has knowledge of the infringement.⁷⁵ On the other hand, OSPs are apt to respond promptly to claims of infringement so that they may enjoy the protection granted by the safe harbor.⁷⁶

To provide effective notice for purposes of the section 512(c) safe harbor, the notification must be a written communication given to the service provider’s designated agent that includes (1) the signature of a person authorized to act on behalf of the copyright owner who alleges his or her copyright work is being infringed; (2) an identification of the copyrighted work in question; (3) an identification of the material alleged to be infringing and information which permits the service provider to locate the material; (4) the contact information for the complaining party; (5) a statement that the complaining party has a good faith belief the material is an unauthorized infringement of a copyrighted work; and (6) a statement under penalty of perjury that the information included in the notice is accurate.⁷⁷

Service providers are further protected by section 512(g)(1), which states that providers will not be held liable for disabling a user’s access or removing any alleged content so long as the provider acted on a good faith basis.⁷⁸ Even if the material in question is ultimately resolved as non-infringing, the service provider will still be insulated from any liability that may be posed by the party affected by the provider’s takedown procedures.⁷⁹

However, if providers seek protection under the section 512(c) safe harbor regarding the material stored on the provider’s system at the direction of the user, the DMCA carves out additional steps that a service provider must take to enjoy the protection offered in section 512(g)(1). These steps include (1) taking “reasonable steps” to give prompt notification to the alleged offending subscriber that their access has been blocked or material removed; (2) providing the purported offending subscriber an opportunity to file counternotice which would contend the claims made in the original

73. CRS REPORT, *supra* note 66, at 7.

74. REPORT OF THE REGISTER OF COPYRIGHTS, *supra* note 16, at 172 n.915.

75. *Id.* at 9.

76. *Id.*

77. 17 U.S.C. § 512(c)(3).

78. *Id.* § 512(g)(1).

79. *Id.*

notice; (3) if counternotice is received, promptly notifying the rights-owner's party that submitted the original notice that a counternotice has been filed; and (4) if the rights-owner does not file legal action seeking to restrain the subscriber's alleged infringing activity within ten days, reinstating the subscriber's access to the system or replace the removed material within ten-to-fourteen business days following the receipt of the counternotice.⁸⁰

Similar to the original notice, the counternotice must be in writing and include (1) the signature of the subscriber; (2) identification of the material that has been removed and the location the material was located prior to removal; (3) a statement under penalty of perjury that the subscriber has a good faith belief that access was disabled or material was removed due to mistake or misidentification; and (4) the contact information of the subscriber as well as a statement consenting to the jurisdiction of the federal district court for the district in which the subscriber's address located.⁸¹ In an attempt to reduce potential abuse of the notice and takedown procedure, if any person "knowingly materially represents" their claims that either a material or activity is infringing (regarding an initial notice) or that material or access was mistakenly removed or revoked (regarding a counternotice), the DMCA holds that person liable for damages, costs, and attorneys' fees incurred by the alleged infringer, the rights-owner, or the service provider.⁸²

II. PROPOSALS TO REFORM THE DIGITAL MILLENNIUM COPYRIGHT ACT

A. THERE ARE TWO COMPETING POLICIES CONCERNING THE EFFICACY OF THE DIGITAL MILLENNIUM COPYRIGHT ACT

The DMCA certainly provides incentives for service providers to heed notices of copyright infringement and take swift action upon receipt of notice.⁸³ However, in the current age of mass digital content creation, the takedown notice regime may also have a negative, sweeping effect on how service providers respond to notices filed against their users.⁸⁴

In recent years, the Copyright Office has held hearings with numerous rightsholders and policymakers testifying to address whether the DMCA has been effective in its goal to balance the liability-mitigating needs of OSPs with the needs of rightsholders for protection over their works.⁸⁵ OSPs

80. *Id.* § 512(g)(2).

81. *Id.* § 512(g)(3).

82. *Id.* § 512(f).

83. REPORT OF THE REGISTER OF COPYRIGHTS, *supra* note 16, at 72–73.

84. *Id.*

85. *Id.*

generally laud the enactment of section 512, pointing to the fact that the strides in innovation and advancement in the digital landscape have come about largely due to the protections that the safe harbor provisions grant OSPs.⁸⁶ On the other hand, rightsholders argue that Title II of the DMCA has done little to protect copyright owners from online infringement.⁸⁷

On June 2, 2020, during a hearing of the Senate Subcommittee on Intellectual Property, a number of rightsholders testified to their experience combatting relentless incidents of digital piracy.⁸⁸ The rightsholders largely spoke to the enormous burden placed on individual copyright owners to scour the internet for any traces of infringing content so that the rightsholder may provide notice pursuant to the DMCA notice requirements.⁸⁹ Don Henley, the drummer for the popular music group Eagles, testified:

There are currently about 6 billion posts on YouTube. About 1 billion unclaimed. 84% contain music. At two minutes per claim it would take 200 million hours to claim them and take them all down. It's an endless game of whack-a-mole . . . Our job is to create music and art, not to police the internet. That's the job of the huge platforms. They claim they're just a conduit—but they engage with that content, can curate it, identify likes and dislikes, but can't seem to identify copyrighted material.⁹⁰

Henley argued that it was not unrealistic to request that OSPs implement systems that take a more proactive approach to policing infringement on their platforms.⁹¹ Henley contended that “[m]any of the platforms have the tools to do it—it’s just beyond their desire. These tech giants are afraid that blocking infringing content will decrease traffic.”⁹² In concluding his testimony, Henley condemned the DMCA as a “relic of a Myspace era in a TikTok world,” and urged reform to improve the system so that creators, many of them small businesses, could better thrive in a “system that recognizes the needs of online participants in a procedure that properly applies the rules and implements today’s technology with an eye

86. *Id.* at 73–74.

87. *Id.* at 77.

88. Kevin Madigan, *Senators and Creators Say Notice and Takedown System Is Broken, While Platforms Blame the System's Failures on Creators*, COPYRIGHT ALLIANCE (June 4, 2020), https://copyrightalliance.org/ca_post/senators-and-creators-say-notice-and-takedown-system-is-broken-while-platforms-blame-creators [https://perma.cc/R2TL-WH2D]; Eileen McDermott, *Third Senate IP Subcommittee Hearing on DMCA: The 'Grand Bargain' Is No Longer Working*, IPWATCHDOG (June 2, 2020), <https://www.ipwatchdog.com/2020/06/02/senate-ip-subcommittee-hearing-dmca-reform-grand-bargain-no-longer-working/id=122124> [https://perma.cc/QV2G-5A5G].

89. *See* McDermott, *supra* note 88.

90. *Id.*

91. *Id.*

92. *Id.*

toward tomorrow.”⁹³

However, imposing stricter guidelines on OSPs for DMCA takedowns may also have a negative effect on individual users, who are at the mercy of the OSPs’ policies regarding repeat infringers.⁹⁴ Twitch, a live-streaming video platform often used by individuals to broadcast their play styles in popular video games, is one such service provider that recently took a strict approach to music copyright infringement claims made against hundreds of the site’s streamers.⁹⁵ After receiving “thousands” of infringement notices from music rightsholders, Twitch responded by deleting all video clips that contained alleged copyrighted music.⁹⁶ An email was subsequently sent to the streamers who were affected, with the following explanation:

We are writing to inform you that your channel was subject to one or more of these DMCA takedown notifications, and that the content identified has been deleted . . . [Twitch] recognize[s] that by deleting this content, we are not giving you the option to file a counter-notification or seek a retraction from the rights holder. In consideration of this, we have processed these notifications and are issuing you a one-time warning to give you the chance to learn about copyright law and the tools available to manage the content on your channel.⁹⁷

Many of the site’s creators did not receive this decision favorably. Prior to the “purge” of the infringing material, many Twitch streamers had received notices that there was at least one copyright strike on clips taken from their streaming videos.⁹⁸ The notices came as quite a surprise to creators, as many of the challenged clips had not been recently uploaded, and streamers had not been given any prior warning that there were such “ticking time bombs” in their content library.⁹⁹

One mechanism Twitch had in place to mitigate copyright infringement claims was a system that automatically muted segments of videos on demand (VOD) containing copyrighted music.¹⁰⁰ However, the system was not adequate to address the creation of “clips,” short segments lasting a minute

93. *Id.*

94. Nathan Grayson, *Twitch DMCA Purge Deletes Thousands of Streamers’ Videos*, KOTAKU (Oct. 20, 2020, 6:30 PM), <https://kotaku.com/twitch-deletes-thousands-of-streamers-videos-and-issues-1845429294> [<https://perma.cc/3FLM-QUQX>].

95. *Id.*

96. *Id.*

97. *Id.*

98. Nathan Grayson, *After Massive DMCA Takedown, Twitch Streamers Are Deleting Thousands of Clips*, KOTAKU (June 8, 2020, 6:30 PM), <https://kotaku.com/after-massive-dmca-takedown-twitch-streamers-are-delet-1843954430> [<https://perma.cc/RDX8-AEZ6>].

99. *Id.*

100. *Id.*

or less, taken from the original video source.¹⁰¹ Clips may be created by any viewer, and clips survive even when the original VOD from which they are pulled is deleted.¹⁰² Many popular streamers' VODs can spawn thousands of clips, and streamers may delete clips associated with a particular VOD.¹⁰³ The problem is that streamers have no way of knowing which clips may contain the copyrighted material flagged in the original VOD, so ultimately, their safest option to avoid a copyright strike or permanent ban is to delete all clips associated with a flagged VOD.¹⁰⁴ Though a seemingly simple solution, e-sports¹⁰⁵ attorney Bryce Blum explains,

The notion that a repeat infringer loses their account is fine in theory but it can't be this devoid of human judgment. . . . It also must be said that the value of a popular Twitch or YouTube channel in today's environment simply wasn't contemplated when the DMCA was written. These aren't just accounts—they're the work product of years of personal investment, dedication, and sacrifice by the creator. A rigid system made a lot of sense when it was created and still does in some contexts, but the DMCA needs to be re-evaluated in light of the modern influencer climate. This is big business, and it deserves more consideration than a judgment-free three strikes and you're out.¹⁰⁶

Twitch has since apologized for the lack of tools offered to its users to protect themselves against copyright infringement claims.¹⁰⁷ Plans are underway to equip the site with better, more user-friendly systems that detect copyrighted audio and provide "more granular ways" for streamers to manage their content libraries.¹⁰⁸ Additionally, Twitch has promised to implement tools that provide streamers more control in reviewing potentially infringing VODs and to allow streamers to review the contested portions of content so that they are more easily able to file counter-notifications under the DMCA.¹⁰⁹ Still, the issues initially borne from Twitch's internal system

101. *Id.*

102. *Id.*

103. *Id.*

104. *Id.*

105. Otherwise known as electronic sports or competitive gaming, e-sports involve professional video game players who compete against one another in broadcasted tournaments, often for cash prizes or brand endorsements. See Kirstin Hallmann & Thomas Giel, *eSports—Competitive Sports or Recreational Activity?*, 21 *SPORT MGMT. REV.* 14 (2017); see also AJ Willingham, *What Is eSports? A Look at an Explosive Billion-Dollar Industry*, CNN (Aug. 27, 2018), <https://www.cnn.com/2018/08/27/us/esports-what-is-video-game-professional-league-madden-trnd/index.html> [<https://perma.cc/L5KU-JQGL>].

106. Grayson, *supra* note 98.

107. Bijan Stephen, *Twitch Apologizes to Streamers for Its Mishandling of Music Copyright*, VERGE (Nov. 11, 2020), <https://www.theverge.com/2020/11/11/21560913/twitch-streamers-dmca-copyright-tools-apology> [<https://perma.cc/4PLV-REK6>].

108. *Id.*

109. *Id.*

may indicate that the DMCA's notice and takedown procedure is showing signs of "wear and tear," perhaps proving to be too antiquated to appropriately address the current policies at play within the digital space.¹¹⁰

While one potential solution to alleviate the burden of rightsholders to police for infringing content is to have OSPs impose a system that flags potential infringement on an automated basis, this approach is still susceptible to "errors and abuses that chill lawful online speech."¹¹¹ YouTube's Content ID system is one example of an internal OSP system, which automatically flags copyrighted material that appears in videos uploaded by its users.¹¹² The system scans videos uploaded to YouTube, comparing them against files of copyrighted works submitted by rightsholders.¹¹³ Rightsholders are notified when the system identifies a match between a third-party's posted material and the rightsholder's copyrighted work; after notification, rightsholders have the option of blocking the video from viewership, running advertisements against the video, or merely tracking the video's viewership numbers.¹¹⁴

Though the system is regarded as quite sophisticated, the very nature of its automation means that it is incapable of discerning whether the use of the copyrighted material is permissible under the fair use doctrine.¹¹⁵ The managers of the New York University ("NYU") School of Law YouTube page provided insight into the process one enters when the Content ID system flags videos for copyright infringement.¹¹⁶ In June 2019, the NYU School of Law YouTube page posted a video recording of a panel hosted at NYU Engelberg Center's Proving IP symposium held in May 2019.¹¹⁷ The panel included two musical experts who explained how they each analyzed songs to prove song similarity in copyright infringement cases.¹¹⁸ The presentation included clips of the songs discussed so that the audience could hear and compare examples of such contested songs.¹¹⁹

110. Thom Tillis, *Getting Back to Basics on the Digital Millennium Copyright Act*, HILL (Dec. 17, 2019, 2:30 PM), <https://thehill.com/blogs/congress-blog/technology/474918-getting-back-to-basics-on-the-digital-millennium-copyright-act> [<https://perma.cc/KA3F-KVWX>].

111. REPORT OF THE REGISTER OF COPYRIGHTS, *supra* note 16, at 11.

112. *How Explaining Copyright Broke the YouTube Copyright System*, NYU SCH. L. ENGELBERG CTR. ON INNOVATION L. & POL'Y, <https://www.law.nyu.edu/centers/engelberg/news/2020-03-04-youtube-takedown> [<https://perma.cc/MGX9-QE85>].

113. Technical Help Page Describing *How Content ID Works*, YOUTUBE, <https://support.google.com/youtube/answer/2797370> [<https://perma.cc/WWC4-428Z>] [hereinafter YouTube Help Page].

114. *Id.*

115. *How Explaining Copyright Broke the YouTube Copyright System*, *supra* note 112.

116. *Id.*

117. *Id.*

118. *Id.*

119. *Id.*

The video was eventually flagged by YouTube's Content ID system due to the use of copyrighted songs in the panel presentation.¹²⁰ Confident that the use of the songs was a textbook example of fair use, NYU officials disputed the claims through the appropriate channels available through YouTube's internal system.¹²¹ Still, one music label that owned the copyright to some of the contested songs, Universal Music Group, responded that even after reviewing NYU's dispute claims, there was still a valid copyright claim.¹²² NYU representatives learned that the YouTube system provided them another opportunity to dispute Universal Music Group's infringement claims, but if their challenge to the infringement claims ended in a loss, the NYU Law YouTube page would suffer "copyright strikes"; multiple strikes can result in the channel being restricted from basic YouTube functions like live-streaming or even terminated altogether.¹²³

The copyright claims were eventually dropped and NYU did not have to continue in its counternotification efforts, but the process highlights the difficulties content creators must face when incorporating copyrighted material into their videos, even when this incorporation is likely protected by fair use.¹²⁴ As the NYU channel managers point out, the system, as sophisticated as it is, still has flaws in flagging material, and though the automatic process certainly expedites monitoring procedures, "the system will still require informed and fair human review at some point."¹²⁵ The Content ID system represents YouTube's unique implementation of a program-specific takedown procedure, and the flagging of a video does not in and of itself constitute a DMCA section 512 takedown notice.¹²⁶ Additionally, Content ID is limited to rightsholders that "own exclusive rights to a substantial body of original material that is frequently uploaded by the YouTube creator community,"¹²⁷ which some have criticized as an unfair exclusion of smaller copyright owners.¹²⁸

The effects of the DMCA on web-based content sharing platforms like Twitch and YouTube suggest that the current digital landscape requires a revamped set of rules that still provide for safe harbor protection while

120. *Id.*

121. *Id.*

122. *Id.*

123. *Id.*

124. *Id.*

125. *Id.*

126. *Id.*

127. YouTube Help Page, *supra* note 113; see also *Qualify for Content ID*, YOUTUBE HELP, <https://support.google.com/youtube/answer/1311402> [<https://perma.cc/5WQD-98M4>].

128. REPORT OF THE REGISTER OF COPYRIGHTS, *supra* note 16, at 43 ("[E]very artist should be entitled to this service, to register their music once and for all.").

addressing the need for more nuanced monitoring systems that are not automatically triggered by any use of copyrighted material.¹²⁹ Though the DMCA accurately anticipated that copyright law required additional revisions with the rise of digital technologies, two decades have passed since its enactment, and the digital landscape may be signaling that it is time for continued revisions to copyright protections as applied to digital works.¹³⁰

B. THE DUTY TO MONITOR AND THE ADOPTION OF A NOTICE AND STAY-DOWN SYSTEM ARE POTENTIAL AREAS OF REFORM

In an extensive report released by the Copyright Office, the resounding conclusion from a series of roundtable discussions with copyright owners, OSP representatives, and policymakers was that “the internet of today is not the internet of 1998.”¹³¹ The current internet landscape involves a “rich tapestry” of social networking sites, online retailers and e-commerce businesses, and platforms that showcase the music and audiovisual entertainment from large record labels, independent artists, and new emerging artists.¹³² Additionally, technological advances have vastly improved internet speeds, such that users now enjoy near-instantaneous search results.¹³³

With the growth of internet services, speed, and access, opportunities for digital piracy have also evolved.¹³⁴ Despite Congress’ intent for the DMCA to provide a balance between protecting the rights of copyright owners and facilitating the further advancements of technological innovation, the Copyright Office ultimately concluded that “Congress’ original intended balance has been tilted askew.”¹³⁵ To address this imbalance, the Copyright Office indicated a number of areas for reform, a selection of which are noted below.¹³⁶

1. The Relationship Between the Knowledge Requirement and the Lack of Imposition of Duty to Monitor Requires Clarification

While section 512(m) clearly states that OSPs are not held to a duty to monitor their platforms for potentially infringing material, this release from a monitoring duty is tempered by the knowledge requirements imposed in

129. Grayson, *supra* note 99; *How Explaining Copyright Broke the YouTube Copyright System*, *supra* note 112.

130. REPORT OF THE REGISTER OF COPYRIGHTS, *supra* note 16, at 28.

131. *Id.*

132. *Id.*

133. *Id.*

134. *Id.*

135. *Id.* at 1.

136. *Id.* at 84.

section 512(c).¹³⁷ Because section 512(c) requires expeditious action to remove infringing material when the OSP has “red flag” knowledge of the infringing activity, the obligations to remain alert to such red flags can appear muddled in light of section 512(m).¹³⁸ The Copyright Office thus noted that “a fuller articulation of the intended balance between [the section 512(m) provision] and other provisions in section 512 would be valuable for stakeholders and courts.”¹³⁹

The Copyright Office has also suggested that an evaluation by Congress regarding the current court interpretations of the common law vicarious liability standard may provide helpful confirmation of whether courts’ interpretations are in line with the balance sought by the DMCA.¹⁴⁰ The test for vicarious liability is largely mirrored in section 512(c)(1)(B), in which OSPs’ eligibility for safe harbor protection hinges on whether the provider “receive[s] a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity.”¹⁴¹ With regards to the “financial benefit” prong, recent litigation has highlighted divergences amongst district courts on how “direct” the benefit has to be.¹⁴² With regards to the “right and ability to control” prong, the court in *Viacom* stated that this prong must be satisfied by a showing of “something more than the ability to remove or block access to materials posed on a service provider’s website.”¹⁴³ Clarification from Congress regarding the application of this two-pronged test may help guide courts in the future and subsequently assist service providers in understanding the scope of the vicarious liability doctrine.¹⁴⁴ Further discussion regarding vicarious liability of ISPs is located in Part IV of this Note.

2. Updating the Digital Millennium Copyright Act with a Notice and Stay-Down System

The Copyright Office has noted the ambiguous statutory language in section 512(c)(3), which requires a rightsholder to include in his or her notice to the OSP “information reasonably sufficient to permit the service provider

137. 17 U.S.C. § 512(c), (m).

138. REPORT OF THE REGISTER OF COPYRIGHTS, *supra* note 16, at 3.

139. *Id.*

140. *Id.*

141. 17 U.S.C. 512(c)(1)(B).

142. *Compare* UMG Recordings, Inc. v. Bright House Networks, LLC, 2020 U.S. Dist. LEXIS 122774, at *16–17 (M.D. Fla. July 8, 2020), *with* Warner Recs. Inc. v. Charter Commc’ns, Inc. 454 F. Supp. 3d 1069, 1083–84 (D. Colo. 2020).

143. *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012) (quoting *Capitol Recs., Inc. v. MP3tunes, LLC*, 821 F. Supp. 2d 627, 645 (2011)).

144. REPORT OF THE REGISTER OF COPYRIGHTS, *supra* note 16, at 4.

to locate” the alleged infringing material.¹⁴⁵ While this requirement has been interpreted as requiring a rightsholder to submit “unique, file-specific URL” addresses to identify every instance of infringing material on an OSP’s service,¹⁴⁶ this interpretation also imposes a significant burden on the rightsholder to closely monitor for infringing activity in a painstakingly time-intensive manner. During the June 2020 Senate IP Subcommittee hearing, Doug Preston, president of the Authors Guild, further explained that the requirement to cite individual URLs in each submitted notice was further frustrated by the fact that oftentimes, the same infringed material would reappear later under a different URL on the same website.¹⁴⁷ Preston, along with other rightsholders, has supported the adoption of a notice and *stay-down* framework, in which a takedown notice “generally triggers a duty for the service provider to proactively identify and remove all instances of the infringing content and prevent future uploads.”¹⁴⁸ The Copyright Office did not explicitly recommend the adoption of a notice and stay-down regime, but it did state that “additional study . . . with public input, would be needed in order to explore the possible contours of any such future proposals.”¹⁴⁹

III. INTERNET SERVICE PROVIDERS AND SECONDARY COPYRIGHT INFRINGEMENT LIABILITY

A. HISTORY OF SECONDARY LIABILITY FOR COPYRIGHT INFRINGEMENT

When an individual violates the Copyright Act by impermissibly infringing on any of the exclusive rights afforded to the copyright owner, the owner may take legal action against the individual on grounds of copyright infringement.¹⁵⁰ However, when seeking action against OSPs for copyright infringement done by individuals subscribed to the service provider, copyright owners must largely rely on the availability of secondary liability claims, rather than direct infringement claims.¹⁵¹ These claims have largely consisted of both contributory liability and vicarious liability.¹⁵²

145. *Id.*

146. *Id.*

147. Madigan, *supra* note 88.

148. *Id.* at 54.

149. *Id.* at 7.

150. *See* 17 U.S.C. § 504(b).

151. Sverker K. Högberg, *The Search for Intent-Based Doctrines of Secondary Liability in Copyright Law*, 106 COLUM. L. REV. 909, 910–11 (2006).

152. *Id.*

1. Contributory Liability Test

Contributory liability infringement may be best encapsulated by the Second Circuit's decision in *Gershwin Publishing Corp. v. Columbia Artists Management, Inc.*¹⁵³ The standard in *Gershwin* established that "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer."¹⁵⁴

Under the *Gershwin* standard, contributory liability claims have been successful in cases where third parties infringed on copyright owners' exclusive right to authorize the performance of a copyrighted work.¹⁵⁵ In *Columbia Pictures Industries, Inc. v. Aveco, Inc.*, a video rental store was held as a contributory infringer due to its practice of charging patrons a fee for viewing copyrighted movies in private viewing rooms.¹⁵⁶ The Third Circuit noted that in the Copyright Act, Congress intended "to avoid any questions as to the liability of contributory infringers. For example, a person who lawfully acquires an authorized copy of a motion picture would be an infringer if he or she engages in the business of renting it to others for purposes of an unauthorized public performance."¹⁵⁷ In *Fonovisa, Inc. v. Cherry Auction, Inc.*, operators of a flea market were held contributorily liable for copyright infringement because they provided reserved spaces for vendors they knew to be selling counterfeit music recordings.¹⁵⁸ The Ninth Circuit followed the reasoning applied in *Columbia Pictures* and agreed that "providing the site and facilities for known infringing activity is sufficient to establish contributory liability."¹⁵⁹

The *Gershwin* rule was further modified in *Sony Corp. of America v. Universal City Studios, Inc.*, in which Sony manufactured home video recorders that some consumers used to film television broadcasts to retain copies for later viewing.¹⁶⁰ The copyright owners of the television programs claimed this was equivalent to providing a means by which infringement could take place, thus constituting contributory liability as it did in *Columbia Pictures* and *Fonovisa*.¹⁶¹ However, the Court held that in situations where

153. *Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162–63 (2d Cir. 1971).

154. *Id.* at 1162.

155. *See Columbia Pictures Indus., Inc. v. Aveco, Inc.*, 800 F.2d 59, 63 (3d Cir. 1986).

156. *Id.* at 61–62.

157. *Id.* at 62 (quoting H.R. REP. NO. 94-1476, at 61 (1976), *reprinted in* 1976 U.S.C.A.N. 5659, 5674).

158. *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264 (9th Cir. 1996).

159. *Id.*

160. *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 419 (1984).

161. *See id.* at 424–25.

the defendant's sole contribution to the infringing activity was the production of the means by which the infringement was carried out, the defendant will not be held contributorily liable if the product "is capable of commercially significant noninfringing uses."¹⁶² Thus, though Sony had produced a videotape recorder that *could* be used to record copyrighted television broadcasts, Sony was not held liable for contributory infringement because the video recorder could also be used for non-infringing activities, such as filming and creating original content.¹⁶³

The modification to *Gershwin* resulted from the concern that holding suppliers of copying technology liable for the infringing activities their products are capable of would drive down the availability of the products.¹⁶⁴ If such suppliers were held liable, technology like digital video recorders and handheld video cameras would not be accessible by the public, thus depriving a societal benefit that is capable of non-infringing use.¹⁶⁵ Similar to these competing policy concerns are the current considerations of whether vicarious liability claims should be available for copyright owners to bring against internet service providers that merely provide the internet service that runs websites or programs where the infringing activity takes place.

The Supreme Court applied the test for contributory infringement against peer-to-peer file-sharing software¹⁶⁶ in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*¹⁶⁷ In *Grokster*, the distributors of software that enabled users to illegally download copyrighted materials argued that the modified contributory liability standard in *Sony* should protect them from any claims of infringement.¹⁶⁸ The distributors argued that they were not liable for the infringing activities of its users because their software had the capacity to serve other, non-infringing activities.¹⁶⁹ However, the Court rejected this argument because several facts indicated that the distributors' knowledge of the infringing activities of its subscribers went beyond simply providing the software on which the infringement was carried out.¹⁷⁰ The

162. *Id.* at 442.

163. *Id.*

164. LAFRANCE, *supra* note 22 at 327–28.

165. *Id.*

166. Peer-to-peer networks, otherwise abbreviated as "P2P networks," allow different computer systems to connect over the internet. P2P, TECHTERMS, <https://techterms.com/definition/p2p> [<https://perma.cc/MH33-GJTQ>]. All that is required to engage in a peer-to-peer network is access to a computer and an internet connection. *Id.* When peer-to-peer software is used, participating computers may share files by allowing each computer within the network to access each other's file systems. *Id.* The convenience of file-sharing is achieved through the advent of these peer networks, but the use of such software programs has greatly contributed to the rise of software piracy and illegal music downloads. *Id.*

167. *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 930 (2005).

168. *Id.* at 922.

169. *Id.* at 922–23.

170. *Id.* at 924–26.

Court identified that the case still involved tension “between the respective values of supporting creative pursuits through copyright protection and promoting innovation in new communication technologies by limiting the incidence of liability for copyright infringement.”¹⁷¹ Despite the consideration that the distributors were merely an advancement of technology that should not be held liable for their infringing users, the distributors’ conduct indicated it had an *inducing* effect on the infringing subscribers, such as promoting their file-sharing system to known infringers, helping subscribers to locate and play copyrighted works, and failing to install any filtering or monitoring system which would have diminished the infringing activity.¹⁷² Thus, *Sony* did not apply because the distributors had not merely supplied a product which was capable of infringing use; rather, the distributors’ actions affirmatively induced the infringing activity: “one who distributes a device with the object of promoting its use to infringing copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.”¹⁷³

2. Vicarious Liability Test

Distinct from contributory liability, vicarious liability for copyright infringement is based on the legal doctrine of respondeat superior.¹⁷⁴ The current standard for determining vicarious liability may also be derived from the court’s ruling in *Gershwin*, which stated that “even in the absence of an employer-employee relationship one may be vicariously liable if he has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities.”¹⁷⁵ Thus, the two-prong test for vicarious liability has since been applied to claims of vicarious liability: (1) the right and ability to supervise, and (2) a direct financial interest.¹⁷⁶

Illustrating the contours of the right and ability to supervise prong, vicarious liability claims will not succeed when there is no evidence to demonstrate the defendant could have intervened in the infringing activity to stop the activity from continuing.¹⁷⁷ Prior to the Supreme Court’s review of *Grokster*, the Ninth Circuit held that the software distributors were not vicariously liable because they “did not monitor or control the use of the software, had no agreed-upon right or current ability to supervise its use, and

171. *Id.* at 928.

172. *Id.* at 938–40.

173. *Id.* at 919.

174. LAFRANCE, *supra* note 22, at 328.

175. *Gershwin Publ’g Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971).

176. *Id.*; *see also* Högberg, *supra* note 151, at 915.

177. *Grokster*, 545 U.S. at 928.

had no independent duty to police infringement.”¹⁷⁸ The failure to meet the right and ability prong may also be seen in *Perfect 10, Inc. v. Visa International Service Ass’n*, in which a credit card servicer processed payments to websites that gave access to infringing material.¹⁷⁹ Though the copyright owners of the infringed material argued that the credit card service processor had control over whether the credit payments would go through, the Ninth Circuit held that though “this refusal would reduce the number of those sales, that reduction is the result of indirect economic pressure rather than an affirmative exercise of contractual rights.”¹⁸⁰ Thus, the *Perfect 10* court noted a distinction between the right and ability to *supervise* and *control*, and the ability to *affect* the infringing activity.

The direct financial benefit prong allows for some attenuation regarding how “direct” the benefit is. For example, the sales of infringing goods at a flea market may financially benefit the owners of the flea market, because although the owners are not receiving a direct cut of the profit from the infringing goods, the results of the popularity of the infringing goods—that is, increased customer traffic and overall increased revenue in concession fees and admission—have still been considered a financial benefit “direct” enough to constitute vicarious liability.¹⁸¹ Similarly, in *Shapiro, Bernstein & Co. v. H.L. Green Co.*, a department store that had hired a “concessionaire” to run a phonograph record department received a direct financial benefit because the department store audience paid admission primarily to listen to the “bootleg” records played by the department.¹⁸²

B. CURRENT STANDARDS FOR SECONDARY LIABILITY ARE LESS CLEAR WHEN APPLIED TO PASSIVE INTERNET SERVICE PROVIDERS

As internet usage grew, opportunities for digital copyright infringement presented a new challenge for the way claims of secondary liability for copyright infringement could be applied to various internet service providers, including access providers, search engines, and online auction sites.¹⁸³ In some cases like *Grokster*, a software provider was held secondarily liable, as its conduct indicated it had taken a more active role in permitting the infringing activity to occur.¹⁸⁴ Similar cases include *A&M*

178. *Id.*

179. *Perfect 10, Inc. v. Visa Int’l Serv. Ass’n*, 494 F.3d 788, 792 (9th Cir. 2007).

180. *Id.* at 805.

181. *Fonovisa Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 263–64 (9th Cir. 1995).

182. *Shapiro, Bernstein & Co. v. H.L. Green Co.*, 316 F.2d 304, 307 (2d Cir. 1963).

183. *LAFRANCE*, *supra* note 22, at 332–33.

184. *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 938 (2005).

*Records, Inc. v. Napster, Inc.*¹⁸⁵ and *In re Aimster Copyright Litigation*,¹⁸⁶ in which file-sharing services were also held secondarily liable as they met the tests for either contributory or vicarious liability.

However, courts struggle more when ISPs play a more passive role in the infringing activity. *Grokster*, *Napster*, and *Aimster* all consisted of facts that showed the software providers were not simply providing a service that consumers then used to engage in infringing activity.¹⁸⁷ The result is not as clear when ISPs serve merely as a conduit for subscribing users. Should ISPs be held to the modified standard stated in *Sony*, where the fact that the infringing activity occurred on the service platform provided by the ISP would not be enough to constitute secondary liability, given that the same services provided by ISPs are also clearly used for non-infringing activity? Should such a sweeping allowance be tempered by placing some responsibility on the ISPs to act against egregious infringing activity? The DMCA currently does not provide clear answers to these questions, but this Note will propose responses in the next Section.

C. “MERE CONDUIT” INTERNET SERVICE PROVIDERS CURRENTLY FACE LITIGATION CONCERNING SECONDARY LIABILITY CLAIMS

Recent litigation shows that copyright owners, particularly large music labels, have brought secondary liability claims against ISPs to court. In April 2020, a Colorado district court judge denied a motion to dismiss filed by defendant Charter Communications, one of the largest ISPs in the country, in a matter brought by Warner Records Inc.¹⁸⁸ Warner Records alleged that Charter should be held vicariously liable for the infringing activity of its subscribers, particularly the actions of individuals who regularly infringed on Warner Records’ copyrighted works through the popular peer-to-peer sharing program BitTorrent.¹⁸⁹ Warner Records argued that the two-prong test for vicarious liability, (1) the right and ability to supervise, and (2) a direct financial interest, had been satisfied because (1) Charter had the ability to terminate its subscribers’ ability to access their internet services, and (2) Charter received a financial benefit from the increased number of subscribers

185. *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1019–20 (9th Cir. 2001).

186. *In re Aimster Copyright Litigation*, 334 F.3d 643, 654 (7th Cir. 2003).

187. *See id.*; *Grokster*, 545 U.S. at 919–26; *Napster*, 239 F.3d at 1011–12.

188. *Warner Recs. Inc. v. Charter Commc’ns, Inc.*, 454 F. Supp. 3d 1069, 1079–80 (D. Colo. 2020).

189. *Id.* The appeal of such peer-to-peer networks is discussed within the opinion, describing BitTorrent as a popular peer-to-peer software program that “facilitates much faster downloading by breaking files into smaller pieces, allowing users to download different pieces from different peers simultaneously. Once a user has downloaded all pieces of a file, the file automatically assembles itself into its complete form and becomes available for playback by the user.” *Id.* at 1080 (citation omitted). The opinion further cites a 2011 report that estimated that 11.4% of all internet traffic involved the illegal pirating and distribution of copyrighted works through BitTorrent alone. *Id.*

who were drawn to its services due to its advertised high-speed internet and apparent failure to terminate internet service for infringing subscribers.¹⁹⁰

Charter argued that the vicarious liability claim should be dismissed because (1) though it has the ability to terminate user accounts, it is not capable of identifying and policing potential infringers, and (2) the financial benefit that Warner Records alleged does not qualify as “direct.”¹⁹¹ Charter argued that because it cannot directly control the infringing actions of its subscribers, it cannot be held to have the requisite ability to supervise or control for a vicarious liability claim.¹⁹² Additionally, Charter characterized Warner Records’ allegations that it advertised high internet speeds as too attenuated of a claim for the purposes of establishing a direct financial benefit.¹⁹³ The district court acknowledged that in a non-binding Ninth Circuit case, *Perfect 10, Inc. v. Giganews, Inc.*, it was held that the “essential aspect of the ‘direct financial benefit’ inquiry is whether there is a causal relationship between the infringing activity and any financial benefit a defendant reaps, regardless of how substantial the benefit is in proportion to a defendant’s overall profits.”¹⁹⁴ Charter interpreted this language to indicate that the draw of infringing activity must be “*the* attracting factor,” but the district court judge disagreed and found that the language could point to the possibility of “*an* attracting factor” being enough to satisfy the direct financial benefit prong.¹⁹⁵

The decision to deny the motion to dismiss was met with concerns that allowing vicarious liability claims would “turn ‘every ISP’ into an infringer.”¹⁹⁶ In fact, in a more recent case, *UMG Recordings, Inc. v. Bright House Networks, LLC*, UMG Recordings brought virtually the same complaint as listed in *Charter* except against another large ISP, Bright House Network (“BHN”), and BHN succeeded in its motion to dismiss the UMG’s vicarious liability claim.¹⁹⁷ When evaluating the vicarious liability claim, the court found that UMG had failed to adequately plead that BHN had received a direct financial benefit.¹⁹⁸ The court noted that UMG relied on non-binding case law that held “to constitute a direct financial benefit, the ‘draw’ of

190. *Id.* at 1080–81.

191. *Id.* at 1084.

192. *Id.* at 1078–79.

193. *Id.* at 1077–78.

194. *Id.* at 1074 (quoting *Perfect 10, Inc. v. Giganews, Inc.*, 847 F.3d 657, 673 (9th Cir. 2017)).

195. *Id.* at 1082.

196. Bill Donahue, *Copyright Professors Raise Alarm over Charter Piracy Case*, LAW360 (Nov. 14, 2019, 3:32 PM), <https://www.law360.com/articles/1219881/copyright-professors-raise-alarm-over-charter-piracy-case> [<https://perma.cc/U7UV-XK3Z>].

197. *UMG Recordings, Inc. v. Bright House Networks, LLC*, 2020 U.S. Dist. LEXIS 122774, at *25 (M.D. Fla. July 8, 2020).

198. *Id.* at *10.

infringement need not be the primary, or even a significant, draw—rather, it need only be ‘a’ draw.”¹⁹⁹ However, the court declined to adopt this interpretation of the direct financial benefit prong, finding that the interpretation “effectively reads the limiting term ‘direct’ out of the test, allowing the imposition of vicarious liability based on indirect, highly attenuated connections between infringing conduct of the patron and alleged financial benefits.”²⁰⁰ Though UMG cited the recent *Charter* decision to argue that, so long as the availability of infringing content was “one among several draws to [the ISP’s] services,” the direct financial benefit prong for vicarious liability could be satisfied, the court declined to adopt as expansive of a reading.²⁰¹

IV. CLARIFIED SAFE HARBOR PROTECTION AND INTERNET SERVICE PROVIDER INSULATION FROM LIABILITY ARE NECESSARY

It is evident that the eligibility requirements for DMCA safe harbor protection have come under scrutiny for their efficacy in achieving the balanced goals of the DMCA. Though the notice and takedown regime was originally envisioned as a collaborative process between OSPs and rightsholders with the common goal to decrease the rampant rates of digital piracy, the statutory framework, to many shareholders, has proven ineffective in achieving this end goal.²⁰² The purpose of this Section is to (1) analyze the effects of current proposals to amend the DMCA, taking into account the main competing policies at play, and (2) argue for a narrow reading of the vicarious liability doctrine as applied to ISPs.

A. ANALYSIS OF PROPOSED AMENDMENTS TO THE DMCA

Several amendments to the DMCA have been suggested by rights-owners and policymakers to clarify the original statutory language that limits OSP copyright infringement liability.²⁰³ Two of these proposals were discussed in Part II of this Note, concerning (1) the clarification between an OSP’s lack of duty to monitor for infringing content under section 512(m) and the knowledge requirements under section 512(c),²⁰⁴ and (2) the possibility of an overhaul of the notice and takedown procedure being

199. *Id.* at *15 (quoting *Arista Recs. LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124, 157 (S.D.N.Y. 2009)).

200. *Id.* at *15–16.

201. *Id.* at *24.

202. REPORT OF THE REGISTER OF COPYRIGHTS, *supra* note 16, at 1.

203. *Id.* at 2–7.

204. *See supra* Section II.B.1.

replaced by a notice and stay-down regime.²⁰⁵

With regards to the seemingly conflicted relationship between the lack of monitoring duty with the requirement to respond expeditiously to red flags that point to infringing behavior, it would be advisable for Congress to clarify whether the prohibition against a duty to monitor includes the lack of an OSP's duty to further investigate red flag knowledge of infringement when such red flag knowledge has not yet achieved a level of specificity to warrant a takedown.²⁰⁶ The Second Circuit has held that there may be some circumstances in which a general knowledge of infringement may suffice as red flag knowledge that would require action on part of the OSP.²⁰⁷ The Second Circuit still asserted that red flag knowledge does not "give rise to an 'amorphous' duty to monitor in contravention of the DMCA," but there still may be some "time-limited, targeted duty—even if encompassing a large number of songs."²⁰⁸ Still, courts have narrowly interpreted what may constitute red flag knowledge, to the point where the Copyright Office noted that participants in a public roundtable held in April 2019 could not identify a single activity that would be "less than actual knowledge but would create red flag knowledge under the current judicial interpretations of the statute."²⁰⁹ Thus, statutory clarification regarding a potential "limited duty to monitor" would prove beneficial to both rightsholders and OSPs: OSPs would have clearer guidance as to when such a duty is triggered, and rightsholders would have increased assurance that the section 512(m) lack of duty to monitor does not minimize an OSP's duty to act expeditiously upon awareness of infringement, whether actual or red flag awareness.²¹⁰

One potential approach to the possibility of a "limited duty to monitor" would be the expansion of automated content-checking software, like YouTube's Content ID system, which could be a required implementation on large sites popularly used for content sharing. Such sites are at risk of pirating activity, and the required implementation of a system that assists copyright owners with monitoring would serve as a way OSPs and copyright owners may collaborate on combating instances of piracy. Additionally, stricter guidelines constituting enforcement against repeat infringers on content sharing sites may be created and implemented, or incentives may be offered for sites to fund the development of more nuanced screening systems.

Though a stricter "limited duty to monitor" approach would prove

205. See *supra* Section II.B.2.

206. REPORT OF THE REGISTER OF COPYRIGHTS, *supra* note 16, at 123–24.

207. EMI Christian Music Grp., Inc. v. MP3tunes, LLC, 844 F.3d 79, 93 (2d Cir. 2016).

208. *Id.*

209. REPORT OF THE REGISTER OF COPYRIGHTS, *supra* note 16, at 123.

210. *Id.*

beneficial, the Copyright Office has recently declined to adopt an extensive overhaul of the current notice and takedown procedure and replace it with a notice and stay-down regime.²¹¹ For the time being, there are still a host of issues that would materialize with the adoption of such a severe approach, namely the level of “match” required between an alleged infringing material and a copyrighted work as well as the glaring implications that a notice and stay-down framework could easily block legitimate speech.²¹² With the example of YouTube’s self-regulated Content ID system, even current monitoring systems are susceptible to flagging videos that would clearly constitute permissible fair use of a copyrighted work.²¹³ However, it is clear that the whack-a-mole problem has unduly placed the impossible burden on rights-owners to monitor OSPs for any appearances of infringing use.²¹⁴ Though OSPs should not be expected to constantly police their platforms for users’ infringing activity, the sheer magnitude and rate at which digital piracy is conducted today cannot be realistically addressed by the original DMCA notice and takedown framework, in which rightsholders are expected to identify every case of infringement of their work to receive any aid from OSP involvement.²¹⁵

Though DMCA’s drafters sought to establish a partnership of sorts between OSPs and rightsholders to combat rising levels of digital piracy, the developments and changes in the virtual landscape within the first two decades of the twenty-first century prove that the weight of responsibility borne by each party in achieving an anti-piracy goal is not appropriately distributed. OSPs as a whole stand in the best position to assist with systematic, sophisticated monitoring of online content, particularly compared with rightsholders that do not have the same breadth of access and ability to review potential infringing activity. Regarding the shortcomings of current content-monitoring systems, OSPs could invest funds to further develop these systems and improve the ease of distinguishing between pirated material and acceptable expressions of fair use. As such, there should be modifications to OSPs’ current lack of a duty to actively monitor for infringed content or repeat infringers on their sharing platforms. The DMCA as it currently stands does not appropriately address rightsholders’ limited capacity to continually screen for instances of their infringed work, nor does

211. Bill Donahue, *Copyright Office Questions Idea of ‘Stay-Down’ System*, LAW360 (July 1, 2020, 3:03 PM), <https://www.law360.com/articles/1287992/copyright-office-questions-idea-of-stay-down-system> [<https://perma.cc/K8D8-SEE4>].

212. *Id.*

213. Elliot Harmon, *‘Notice-and-Stay-Down’ Is Really ‘Filter Everything,’* ELEC. FRONTIER FOUND. (Jan. 21, 2016), <https://www.eff.org/deeplinks/2016/01/notice-and-stay-down-really-filter-everything> [<https://perma.cc/7HDH-CHWK>].

214. Madigan, *supra* note 88.

215. REPORT OF THE REGISTER OF COPYRIGHTS, *supra* note 16, at 77–82.

it provide any incentive for OSPs to shoulder more burden in taking down impermissible copyright use. Modifications to the language of the DMCA would help to better address these issues as more rightsholders call upon legislators for improved protection of their works in the unwieldy depths of the internet space.

B. A NARROW READING OF VICARIOUS LIABILITY DOCTRINE APPLIED TO ISPS

A large portion of this Note has been dedicated to a general review of DMCA safe harbors and the limitations on liability they afford OSPs. However, in instances where an OSP does not qualify for safe harbor protection, the OSP may still be held liable for copyright infringement under common law liability schemes such as direct, contributory, and vicarious liability.²¹⁶ As discussed in Part IV of this Note, recent litigation in district courts has shown different approaches to interpreting the vicarious liability standard applied to ISPs that simply provide their users with access to the internet, acting as “mere conduits” for the online activities conducted by their users.

As noted in an amicus brief filed by copyright law professors in the *Charter* matter, a proper application of the vicarious liability test as applied to ISPs should require the infringing activity to be the main “draw” that attracts infringing subscribers to the ISP in order to satisfy the “direct financial benefit” prong of the vicarious liability test.²¹⁷ Allowing the “direct financial benefit” prong to be satisfied by equating access to high-speed internet as “a” draw significantly lowers the bar to sufficiently state a vicarious liability cause of action.²¹⁸ Doing so would “impose unprecedented risks of liability,” which in turn could harm ISPs, individual users, and the public at large.²¹⁹ Unlike OSPs that serve as hosts for user material, ISPs are “mere[] conduits” that are more akin to telephone or power companies.²²⁰ If ISPs were held to qualify for vicarious liability simply because they advertise fast internet speeds and have the limited ability to terminate service and thereby “control” alleged infringing subscribers, ISPs could be incentivized

216. See, e.g., *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 434–35 (1983) (“The Copyright Act does not expressly render anyone liable for infringement committed by another.”); *id.* at 486 (Blackmun, J., dissenting) (“It is well established that liability of copyright infringement can be imposed on persons other than those who actually carry out the infringing activity.”).

217. Brief Amici Curiae of Copyright Law Professors in Support of Defendant’s Objection to Magistrate’s Recommendation at 1–2, *Warner Recs. Inc. v. Charter Commc’ns, Inc.*, 454 F. Supp. 3d 1069 (D. Colo. 2020) (No. 19-CV-00874).

218. *Id.*

219. *Id.*

220. *Id.*

to “over-enforce and over-deter possible infringing activity” in order to avoid vicarious liability.²²¹ Adopting such a draconian approach to monitoring user activity would have significant impacts on access to internet services—access that individuals rely on daily for “communication, public discourse, work, education, commerce, civic participation, and more.”²²²

Despite a potential need for OSPs to take a more active role in infringement policing through “limited duty to monitor” red flags that point to infringing material, OSPs and “mere conduit” ISPs are clearly distinct from one another, as evidenced by the differing “service provider” definitions provided in the DMCA.²²³ Rightsholders like the large music recording labels seeking secondary liability claims against mere conduit ISPs may certainly require reworked DMCA provisions that afford them improved protections against the relentless onslaught of digital piracy.²²⁴ However, the applicability of the vicarious liability doctrine to mere conduit ISPs appears to be an overreach of rightsholders’ search for redress, which could largely result in undesirable effects on ISP monitoring policies and users’ privacy. Such an overreach is what the drafters of the DMCA sought to prevent so that developments and innovations of the quickly broadening virtual landscape need not be restricted to a fault.

CONCLUSION

Clearly, the current internet landscape has yielded a great number of innovations that have markedly changed the day-to-day workings of individuals compared to the technology available at the time the DMCA was promulgated. Internet access has grown fast, reliable, and ubiquitous; it is available at most individuals’ fingertips daily. With such innovations, the ability to pirate digital works has also evolved to a point where copyright owners must remain vigilant to battle the relentless incidents of infringement that occur with ease in a digital landscape.

While rights-owners in 1998 may have been able to keep up with providing notices to OSPs regarding the discovery of infringing material, rights-owners as of 2020 are no longer equipped to adequately monitor all occurrences of infringement. Creators without the means to continuously scrub the depths of the internet for instances of pirated works are left with very little protection offered from the DMCA. Thus, updated revisions to the DMCA safe harbor limitations are advisable given the current challenges in

221. *Id.*

222. *Id.*

223. *See* 17 U.S.C. § 512(k).

224. REPORT OF THE REGISTER OF COPYRIGHTS, *supra* note 16, at 77–82.

a digital landscape unimagined by the drafters of the DMCA.

However, this conclusion does not necessarily result in the stance that vicarious liability claims as recently seen against ISPs should stand. Vicarious liability claims should still not be imputed to “mere conduit” ISPs, lest ISPs are incentivized to unduly monitor their users’ activity in order to avoid the threat of such liability. The need for an improved DMCA, coupled with the continued recommendation to limit the liability of ISPs for infringing activity conducted by their users, reflects the ongoing effort to achieve the underpinning goal of copyright law: striking the balance between protecting the rights of copyright owners and facilitating continued innovations for future technologies yet to be imagined.