

Columbia Law School

Scholarship Archive

Kernochan Center for Law, Media, and the Arts

Research Centers & Programs

2015

**Robots, Pirates, and the Rise of the Automated Takedown
Regime: Using the DMCA to Fight Piracy and Protect End Users**

Zoe Carpou

Follow this and additional works at: https://scholarship.law.columbia.edu/law_media_arts



Part of the [Intellectual Property Law Commons](#)

Robots, Pirates, and the Rise of the Automated Takedown Regime: Using the DMCA to Fight Piracy and Protect End-Users

Zoe Carpou*

Introduction.....	552
I. Statutory Background and the Current Case Law on Robo-Takedowns	556
A. History and Purpose of the Digital Millennium Copyright Act.....	556
1. Overview.....	556
2. The Section 512(c) Takedown Procedure.....	557
3. The Section 512(g) Counter-Notification Procedure.....	558
B. “Robo-Takedown” Defined.....	559
1. The “Whack-a-Mole” Problem: The Evolution of Robo-Takedowns in Response to High Volume Repeat Offenders.....	559
2. Standard for Determining “Abusive” Takedown Regimes.....	559
C. Evolution of the Section 512(f) Misrepresentation Standard....	561
1. <i>Diebold</i>	561
2. <i>Rossi</i>	562
3. <i>Lenz</i>	563
II. The Problematic Notice-and-Takedown Environment of Today	564
A. Defining the “Problem” of Robo-Takedowns.....	564
1. Overbroad Takedown Requests	565
2. Lack of User Pushback	566
B. Determining the Scope of the Problem	567
1. Urban and Quilter Study	569
2. Seng Study	570
3. The Takedown Project.....	572
4. The NYU Counter-Notification Study.....	572

* J.D. Candidate, Columbia Law School, Class of 2016. I would like to thank Professor Jane Ginsburg for her infinite wisdom and guidance in the drafting of this Note; Professor Tim Wu for his help in choosing a topic and for teaching me copyright law; the entire 2014–15 and 2015–16 editorial staffs of the *Columbia Journal of Law & the Arts* for being an incredible support network; and my friends and family for their endless encouragement—and their understanding of missed phone calls and cancelled plans—as this Note was being produced.

C. Empirical Analysis of Litigation Arising from Potential Misuse of the Notice-and-Takedown Procedure	573
1. Limitations	574
2. Methodology	574
3. Findings	575
III. Harnessing Robots as a Force for Good	583
A. Drawing a Better Line Between “Abusive” and “Non- Abusive” Takedown Practices	584
B. Strengthening the Counter-Notification System with User Education and Empowerment	585
C. Employing Technology to Create More Cost-Efficient “Stay Down” Mechanisms	587
Conclusion	588

INTRODUCTION

This very second, a battle between robots and pirates is being waged online. Pirates are stealing content from copyright holders and uploading it to various websites. Robots are crawling the Web, searching for pirated content. When a robot encounters pirated content, it is programmed to attack—either by reporting back to the copyright holder, or by going straight to the source and requesting that the material be removed. Sometimes the pirates fight back, re-posting the content online soon after it is taken down or posting newly infringing content. The cycle continues, and the battle rages on.¹

Generally speaking, “robots” like the one described above operate in a certain sequence.² First, they scan the Internet for certain keywords or other indicia of copyrighted content. Once the robot locates content it has identified as copyrighted, it informs the copyright holder, who then decides how to react. The copyright holder may investigate the lead further, and, if the content is indeed found to be infringing, may send a request to the Internet service provider (“ISP”) to remove the infringing content. This action is known as a “takedown” or “notice-and-takedown” request.

The robot, however, can also initiate what is known as a “robo-takedown” by contacting the host site directly and requesting that the content be removed.³ By definition, robo-takedown requests are issued pursuant to a largely—if not fully—

1. This particular phenomenon, referred to as the “whack-a-mole problem,” will be explored in greater detail in Part I.B(1).

2. The term “robot” will be used throughout this Note to refer to search algorithms employed to scan the Web for specific indicia of infringing activity.

3. A variety of other terms are also used to describe the same process, including “automated takedown.” See, e.g., Michael W. Carroll, *Pinterest and Copyright’s Safe Harbors for Internet Providers*, 68 U. MIAMI L. REV. 421 (2014).

automated review process, meaning that there is no human actor reviewing the content to verify that it is in fact copyrighted before requesting that it be removed.⁴ Since each takedown request can identify an infinite number of sources pointing to content the algorithm has identified as infringing, this process can sometimes target content that is, in fact, noninfringing.⁵

The intention behind robo-takedown regimes is to combat rampant online piracy, which, while difficult to quantify with exactitude, has been estimated to cost copyright holders billions of dollars annually.⁶ The U.S. Copyright Office recently noted: “the volume of infringing material accessed via the internet more than doubled from 2010 to 2012, and . . . nearly one-quarter of all internet bandwidth in North America, Europe, and Asia is devoted to hosting, sharing, and acquiring infringing material.”⁷

Pirating is also a lucrative endeavor; a 2014 study sponsored by the Digital Citizens Alliance found that websites featuring pirated content rake in over \$200 million annually from advertising revenue and that profit margins on these sites can range anywhere from 80 to 94 percent.⁸

Despite the fact that robo-takedown regimes are employed to combat online piracy, the literature and popular media attention surrounding takedown regimes frequently refer to the “abusive” nature of such practices.⁹ With the proliferation of

4. It should be noted that copyright holders and ISPs alike do not readily disclose the extent to which their processes are automated. For the sake of this Note, the term “robo-takedown” will refer to processes that result in the removal of content online where there is no human actor on either the copyright holder or ISP end verifying that the content is, in fact, infringing. The author makes no claim as to the prevalence of such processes.

5. The term “noninfringing” will be used throughout this Note to refer to content that is uncopyrightable, not copyrighted (e.g., the copyright term has expired), subject to a copyright exception like fair use, or otherwise outside the ambit of federal copyright protection. No attempt will be made to distinguish between these different types of content.

6. See, e.g., Carl Bialik, *Putting a Price Tag on Film Piracy*, WALL ST. J. (Apr. 5, 2013, 11:42 PM), <http://blogs.wsj.com/numbers/putting-a-price-tag-on-film-piracy-1228/> [https://perma.cc/ZC33-EFFH] (comparing studies that found annual losses of between \$6.1 billion and \$20.5 billion); see also Dirs. Guild of Am., *Piracy by the Numbers*, DGA Q. (2010), <https://www.dga.org/Craft/DGAQ/All-Articles/1001-Spring-2010/Internet-Issues-Piracy-Statistics.aspx> [https://perma.cc/Z98S-6LRX] (reporting that global piracy costs U.S. companies \$25 billion in lost sales).

7. Section 512 Study: Notice and Request for Public Comment, 80 Fed Reg. 81862-01 (Dec. 31, 2015).

8. Digital Citizens Alliance, *Good Money Gone Bad: Digital Thieves and the Hijacking of the Online Ad Business* (Feb. 2014), <https://media.gractions.com/314a5a9abbbbc5e3bd824cf47c46ef4b9d3a76/4af7db7f-03e7-49cb-aeb8-ad0671a4e1c7.pdf> [https://perma.cc/67BC-ASKQ].

9. See, e.g., Grant Gross, *What's the problem with DMCA takedown notices?*, PCWORLD (Mar. 20, 2014), <http://www.pcwORLD.com/article/2110520/whats-the-problem-with-dmca-takedown-notices.html> [https://perma.cc/2BKU-GSZP] (“Any multistakeholder dialog that was talking about the notice-and-takedown system and trying to improve it that didn’t include a discussion of takedown abuse would really have no legitimacy in the eyes of many, many Internet users.”); Mike Masnick, *If We’re Going to Change DMCA’s ‘Notice & Takedown,’ Let’s Focus on How Widely It’s Abused*, TECHDIRT (Mar. 14, 2014, 1:36 PM), <https://www.techdirt.com/articles/20140314/11350426579/if-were-going-to-change-dmcas-notice-takedown-lets-focus-how-widely-its-abused.shtml> [https://perma.cc/GA95-LZK2]; Mitch Stoltz, *In Hotfile Docs, Warner Hid References to ‘Robots’ And Its Deliberate Abuse of*

user-generated content (“UGC”)¹⁰ made possible by sites such as YouTube, algorithms have the potential to detect content uploaded not just by seasoned pirates but also by those who have no intention of pirating copyrighted content. And, because of the high volume of takedown requests ISPs receive¹¹ and the speed with which they are required to respond,¹² takedown requests sometimes result in the removal of noninfringing content.¹³ Thus, while it is efficient for copyright holders to move toward automated processes—and many of them are¹⁴—it is also easier for observers to paint such practices as abusive when noninfringing content is removed as a result of a robo-takedown request.

However, the term “abuse” as it pertains to takedown regimes has never been adequately defined. Surely some of the content targeted by takedown requests is actually infringing, and thus robo-takedowns, at least in part, achieve the goal of protecting copyright holders by keeping pirated content off the Web. However, it is also clear that at least in some instances, robo-takedown requests have a chilling effect on free speech by preemptively removing content that does not violate

Takedowns, ELEC. FRONTIER FOUND. (Oct. 9, 2014), <https://www.eff.org/deeplinks/2014/10/hotfile-docs-warner-hid-references-robots-and-its-deliberate-abuse-takedowns> [<https://perma.cc/9Z2D-WEVL>]; Jamie Williams, *Absurd Automated Notices Illustrate Abuse of DMCA Takedown Process*, ELEC. FRONTIER FOUND. (Feb. 24, 2015), <https://www.eff.org/deeplinks/2015/02/absurd-automated-notices-illustrate-abuse-dmca-takedown-process> [<https://perma.cc/97FJ-2AYW>].

10. “UGC sites rely on their users to contribute content. Blogs, wikis, social-networking sites, and video-sharing sites (e.g., YouTube) are among the most popular UGC technologies.” Michael S. Sawyer, Note, *Filters, Fair Use & Feedback: User-Generated Content Principles and the DMCA*, 24 BERKELEY TECH. L.J. 363, 363 (2009).

11. “Google, which as a provider of ‘information location tools’ under the DMCA may receive more takedown requests than any other entity, reports that the number of such requests it receives for Google Search on a weekly basis has climbed into the millions.” INTERNET POLICY TASK FORCE, DEP’T OF COMMERCE INTERNET POLICY TASK FORCE, COPYRIGHT POLICY, CREATIVITY, AND INNOVATION IN THE DIGITAL ECONOMY 57 (2013) [hereinafter COPYRIGHT GREEN PAPER]. There is also evidence that the volume of takedown requests has been increasing year after year. For example, the number of links Google was asked to remove from its search engine in 2014 was a 75% increase from the number of links it was asked to remove the year before. Ernesto Van der Sar, *Google Asked to Remove 345 Million ‘Pirate’ Links in 2014*, TORRENTFREAK (Jan. 5, 2014), http://torrentfreak.com/google-asked-remove-345-million-pirate-links-2014-150105/?utm_source=dlvr.it&utm_medium=twitter [<https://perma.cc/WH2E-K4K4>].

12. See 17 U.S.C. § 512(c)(1)(A)(iii) (2010). This provision of the DMCA will be explored in more depth in section I.A of this Note.

13. For example, Google’s reported compliance with takedown requests for Search is around 97%. Google, *Google Transparency Report*, <http://www.google.com/transparencyreport/removals/copyright/faq/> [<https://perma.cc/6CMV-3FHM>] (last visited Jan. 14, 2015). Note, however, that information regarding the rate with which ISPs comply with takedown requests, the number of requests they receive, and the process by which they comply with such requests is not readily available.

14. “Because the large amount of infringing content on the Internet makes individual review of each item infeasible, large right holder organizations find it necessary to use automation.” COPYRIGHT GREEN PAPER, *supra* note 11, at 57; see also Matthew Schonauer, Note, *Let the Babies Dance: Strengthening Fair Use and Stifling Abuse in DMCA Notice-and-takedown Procedures*, 7 I/S: J. L. & POL’Y FOR INFO. SOC’Y 135, 156 (2011) (“Increasingly, copyright owners look to automate solutions to the demanding task of policing the Internet for infringing uses of their works.”).

anyone's copyright.¹⁵ While some are inclined to find takedown processes abusive by their very nature, particularly with regard to robo-takedowns,¹⁶ others argue that there is only a certain point at which they become so.¹⁷ Adding to the confusion, there is no definitive data on how much of the content that is removed pursuant to robo-takedown requests is actually infringing and the portion of that content that is noninfringing. Some sources suggest that the amount of noninfringing content that is removed is "miniscule" compared to the amount of infringing content that is targeted—a suggestion, perhaps, that the notice-and-takedown system is largely effective.¹⁸ So when, exactly, does a robo-takedown regime move away from its goal of thwarting copyright infringement and become abusive?

This Note argues that automated notice-and-takedown processes are in fact the most efficient means available to deal with the high volume of infringing content in the digital world, but that the counter-notification procedure needs to be strengthened to provide more protection to noninfringing users in the event that their content is removed. Further, the process of scanning for and identifying infringing content must be improved to lessen the incidence of overbroad requests. Part I of this Note provides background on the Digital Millennium Copyright Act ("DMCA") and the evolution of the notice-and-takedown procedure. Part II outlines the problems with the current state of the notice-and-takedown environment, provides an overview of the data available on takedown requests, and presents an empirical analysis of all known litigation arising from user pushback¹⁹ on such requests in an attempt to shed new light on the amount of noninfringing content that is actually targeted. The overarching aim of Part II is to help answer the question of whether takedown requests, generally speaking—but with an emphasis on robo-takedown requests—tend to be abusive in practice, or if instances of overbroad requests are the exception rather than the norm. Finally, Part III suggests ways in which automated notice-and-takedown processes can be refined to strike a better balance between copyright holders, ISPs, and the general public.

15. 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 (2010).

16. See, e.g., Lydia Pallas Loren, *Deterring Abuse of the Copyright Takedown Regime by Taking Misrepresentation Claims Seriously*, 46 WAKE FOREST L. REV. 745, 747 (2011); Schonauer, *supra* note 14, at 156; Williams, *supra* note 9 ("Sending automated notices, without human review, is itself an abuse of the DMCA takedown process.").

17. See, e.g., Cattleya M. Concepcion, Note, *Beyond the Lens of Lenz: Looking to Protect Fair Use During the Safe Harbor Process Under the DMCA*, 18 GEO. MASON L. REV. 219, 232 (2010) (arguing that takedown regimes become abusive when used to suppress fair use).

18. Gross, *supra* note 9 ("[W]hen you look at the number of incorrect or abusive notices in perspective, it's actually a miniscule percentage of the total.").

19. The term "user pushback" will be used throughout this Note to refer to the general process of disputing takedown requests. This can include either counter-notification under 17 U.S.C. § 512(g)(3) or litigation.

I. STATUTORY BACKGROUND AND THE CURRENT CASE LAW ON ROBO-TAKEDOWNS

A. HISTORY AND PURPOSE OF THE DIGITAL MILLENNIUM COPYRIGHT ACT

1. Overview

In 1996, the World Intellectual Property Organization (“WIPO”) enacted a Copyright Treaty, the terms of which apply to all signatory nations, including the United States.²⁰ Congress enacted the DMCA in 1998 to comply with WIPO and to bring the Copyright Act into the digital age.²¹ According to the statute’s legislative history, Congress had two goals in creating the DMCA: “the protection of intellectual property and the promotion of the growth and development of electronic commerce.”²² These goals arose in part out of Congress’s concern about widespread piracy made possible by the rise of digital media.²³

The DMCA added several important features to the preexisting copyright law, including anti-circumvention measures and a statutory safe harbor for UGC sites.²⁴ This latter measure, codified in § 512 of the DMCA, was designed to protect ISPs from liability for copyright infringement for content uploaded on their sites by users so long as the ISPs implement a mechanism designed to remove infringing content.²⁵ Section 512, thus, effectively struck a compromise between ISPs and copyright holders, leading to the rise of UGC sites such as YouTube and Twitter.²⁶

Since enactment of the DMCA in 1998, ISPs have been able to escape liability for infringing material posted by users by complying with a notice-and-takedown procedure, which requires that they remove content “expeditiously” from their sites after receipt of a proper takedown request from a copyright holder.²⁷ By striking a balance between the needs of copyright holders to protect their intellectual property and the need for ISPs to escape liability in order to create innovative technologies, this statutory safe harbor has allowed UGC sites to proliferate and persist.²⁸

It should be briefly noted that some potential forms of online piracy fall outside of the notice-and-takedown structure altogether, specifically because there is no posted content to be taken down. Illegal peer-to-peer file-sharing, for example, is

20. Jeffrey Cobia, Note, *The Digital Millennium Copyright Act Takedown Notice Procedure: Misuses, Abuses, and Shortcomings of the Process*, 10 MINN. J.L. SCI. & TECH. 387, 387–88 (2009).

21. *Id.* at 388.

22. Charles W. Hazelwood, Jr., *Fair Use and the Takedown/Put Back Provisions of the Digital Millennium Copyright Act*, 50 IDEA 307, 308 (2010) (internal quotations omitted).

23. *Id.* at 308.

24. 17 U.S.C. §§ 101–1332 (2010).

25. Rebecca Alderfer Rock, Comment, *Fair Use Analysis in DMCA Takedown Notices: Necessary or Noxious?*, 86 TEMP. L. REV. 691, 693 (2014).

26. *Id.* at 692.

27. 17 U.S.C. § 512(c)(1)(A)(iii) (2010).

28. David Kravets, *10 Years Later, Misunderstood DMCA is the Law That Saved the Web*, WIRED (Oct. 27, 2008), <http://www.wired.com/2008/10/ten-years-later/> [https://perma.cc/8MR4-PBBU].

an ongoing problem that involves piracy that occurs between individual users without any content being posted to the Web.²⁹ New streaming technologies also allow for potential copyright violation that falls outside the ambit of the notice-and-takedown structure. These technologies allow users to stream content live without actually posting anything online that could be the subject of a takedown notice.³⁰ As these activities fall outside the scope and purpose of this Note they will not be explored further.

2. The Section 512(c) Takedown Procedure

Section 512(c) of the DMCA allows ISPs to escape liability for copyright infringement if they comply with a notice-and-takedown procedure by removing allegedly infringing content from their sites in response to takedown requests issued by copyright holders.³¹ Section 512(c)(3)(A) provides six elements that a copyright holder must fulfill in order to effectuate a valid takedown request:

- (i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
- (ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
- (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.
- (iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.
- (v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
- (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.³²

Notably, § 512(c) requires only that the issuer of the takedown request have a

29. Robert Steele, *If You Think Piracy is Decreasing, You Haven't Looked at the Data*. . . ., DIGITAL MUSIC NEWS (July 16, 2015), <http://www.digitalmusicnews.com/2015/07/16/if-you-think-piracy-is-decreasing-you-havent-looked-at-the-data-2/> [https://perma.cc/C4W4-KPY4].

30. See, e.g., Caitlin Dewey, *The future of online piracy is easy, free and already in your pocket*, WASH. POST (Apr. 15, 2015), <https://www.washingtonpost.com/news/the-intersect/wp/2015/04/15/the-future-of-online-piracy-is-easy-free-and-already-in-your-pocket/> [https://perma.cc/F9UY-5NHT].

31. 17 U.S.C. § 512(c) (2010).

32. *Id.* § 512(c)(3)(A)(i)–(vi).

“good faith belief” that the targeted material is actually infringing.³³ The lack of explanation in the statute for what constitutes a “good faith belief” has been the subject of much discussion and litigation.³⁴

3. The Section 512(g) Counter-Notification Procedure

Once a takedown request is issued, the ISP must “take[] reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material[.]”³⁵

Section 512(g)(3) then provides a procedure by which users can push back on takedown requests to either prevent ISPs from taking their content down, or to have their content restored.³⁶ The section details four steps a user must take to serve a counter-notification upon an ISP:

(3) Contents of counter notification.—To be effective under this subsection, a counter notification must be a written communication provided to the service provider’s designated agent that includes substantially the following:

(A) A physical or electronic signature of the subscriber.

(B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled.

(C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.

(D) The subscriber’s name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber’s address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person.³⁷

The amorphous “good faith belief” standard appears again in this section, here as a requirement of the user. What is more, the user must submit to the jurisdiction of the court for any ensuing litigation, a requirement that has no analogue in § 512(c).³⁸

Once the ISP has received the counter-notification, it must notify the original issuer of the takedown notice and replace the content within ten to fourteen

33. *Id.* § 512(c)(3)(A)(v).

34. *See, e.g., Rossi v. Motion Picture Ass’n of America Inc.*, 391 F.3d 1000 (9th Cir. 2004) (discussed *infra* Part I.C.2).

35. 17 U.S.C. § 512(g)(2)(A).

36. *Id.* § 512(g)(3).

37. *Id.* § 512(g)(3)(A)–(D).

38. *Id.* § 512(g)(3)(C)–(D).

business days.³⁹ Replacement of the content, however, is not required if the ISP first receives notice that the copyright holder has filed an action seeking an injunction against the user from engaging in allegedly infringing activity related to the contested content.⁴⁰ Once a counter-notification is issued, the copyright holder, therefore, has the choice to either allow the content to go back up or to file an infringement action against the user.⁴¹

B. “ROBO-TAKEDOWN” DEFINED

“Robo-takedowns” refer to the processes by which copyright holders send automated takedown requests to ISPs after employing algorithms to crawl the Web for indicia of potentially infringing material.⁴² These types of notices can be voluminous, sometimes requesting the takedown of hundreds or even thousands of instances of allegedly infringing content at a time.

1. The “Whack-a-Mole” Problem: The Evolution of Robo-Takedowns in Response to High Volume Repeat Offenders

Robo-takedowns are a fairly recent phenomenon. They evolved in response to what has been described as the “whack-a-mole” problem: once infringing content is removed, there are no mechanisms in place to ensure that it “stays down.”⁴³ The DMCA requires ISPs to implement reasonable policies to deal with repeat infringers, but it is often difficult if not impossible for ISPs to respond adequately to instances in which the same content reappears in high volume, either from the same infringer or from different infringers. Because infringing content can essentially pop back up again right after being removed, the implementation of robo-takedown regimes has become an ever-increasing means of responding to the constant resurgence of infringing material.⁴⁴

2. Standard for Determining “Abusive” Takedown Regimes

Currently, there is no clear standard for determining when a takedown request or regime becomes “abusive.” The term “abuse” as it pertains to takedown regimes is used frequently and amorphously, and the contours of the term have never been

39. *Id.* § 512(g)(2)(B)–(C).

40. *Id.* § 512(g)(2)(C).

41. Rock, *supra* note 25, at 693.

42. *See supra* note 3.

43. “Rights holders report that they find themselves in a game of ‘whack-a-mole’—a never-ending cycle of sending notices about infringing content that may be taken down, only to reappear a short time later in a new location on the same website.” COPYRIGHT GREEN PAPER, *supra* note 11, at 56.

44. Rock, *supra* note 25, at 694 (noting the “onerous” burden the DMCA places on copyright holders to “police the Internet” for instances of infringement while ISPs that are compliant with § 512(c) remain free from liability).

explicitly defined.⁴⁵ For example, it can be applied categorically to any takedown resulting from the use of automated processes.⁴⁶ The term can also arise any time a takedown request stifles speech or gives rise to the specter of censorship, even where such effect is not the goal of the copyright holder.⁴⁷ Yet another application occurs where the issuer of the takedown request is not actually the holder of the copyright in question, or where the takedown notice targets noninfringing content.⁴⁸ The most obvious example is where takedown notices are used as a “sword” rather than as a “shield,”⁴⁹ including blatant attempts to censor criticism or stifle competition.⁵⁰

The closest the actual text of the DMCA gets to delineating a line at which a takedown regime becomes abusive is in § 512(f), which attempts to guard against “knowing material misrepresentations” in the issuance of takedown requests.⁵¹ Indeed, in *Lenz v. Universal Music Corp.*, a case involving user pushback on a robo-takedown request, the court posited that “[t]he purpose of Section 512(f) [of the DMCA] is to prevent the *abuse* of takedown notices.”⁵²

Pursuant to § 512(f), if a copyright holder is found to have knowingly materially misrepresented the infringing nature of a targeted work, she can be held liable for pecuniary damages. Conversely, a user who follows the counter-notification procedure and makes a “willful misrepresentation” as to the noninfringing nature of her work can also be liable for damages.⁵³ The language of § 512(f) reads as follows:

(f) Misrepresentations.—Any person who knowingly materially misrepresents under this section—

(1) that material or activity is infringing, or

(2) that material or activity was removed or disabled by mistake or misidentification,

shall be liable for any damages, including costs and attorneys’ fees, incurred by the alleged infringer, by any copyright owner or copyright owner’s authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed

45. See, e.g., *supra* note 9.

46. See, e.g., *supra* note 16.

47. Cobia, *supra* note 20, at 392.

48. *Id.* at 391–92.

49. See Online Policy Grp. v. Diebold, 337 F. Supp. 2d 1195, 1204–05 (N.D. Cal. 2004).

50. See, e.g., Mike Masnick, *If We’re Going to Change DMCA’s ‘Notice & Takedown,’ Let’s Focus On How Widely It’s Abused*, TECHDIRT (Mar. 14, 2014), <https://www.techdirt.com/articles/20140314/11350426579/if-were-going-to-change-dmcas-notice-takedown-lets-focus-how-widely-its-abused.shtml> [<https://perma.cc/QF3U-P9JR>].

51. In fact, some commentators already associate takedown “abuse” with § 512(f). See, e.g., COPYRIGHT GREEN PAPER, *supra* note 11, at 57.

52. 572 F. Supp. 2d 1150, 1156 (N.D. Cal. 2008) (emphasis added).

53. See *Shropshire v. Canning*, No. 10-CV-01941, 2011 WL 90136 *6 (N.D. Cal. Jan. 11, 2011).

material or ceasing to disable access to it.⁵⁴

The evolution of the § 512(f) standard, which is outlined in more detail below, provides some useful insight into how courts have viewed overreaching notice-and-takedown practices. The contours of what constitutes an abusive takedown practice, however, remain unclear.

C. EVOLUTION OF THE SECTION 512(F) MISREPRESENTATION STANDARD

The § 512(f) standard has evolved over time in response to instances of user pushback on takedown requests, beginning with *Online Policy Group v. Diebold*.⁵⁵ While the standard today remains unclear in most circuits, the following cases provide insight into how courts have dealt with the use and misuse of the notice-and-takedown procedure, which in turn could shed light on how courts will deal with litigation arising from robo-takedowns.

1. *Diebold*

The first case involving a potential misuse of the notice-and-takedown system was *Online Policy Group v. Diebold*.⁵⁶ A group of students at Swarthmore College sued Diebold, a manufacturer of electronic voting machines, for a declaratory judgment that they did not infringe Diebold's copyright, and for injunctive relief arising from Diebold's violation of § 512(f).⁵⁷ Diebold's voting machines had been the subject of public controversy since "the reliability and verification procedures of the machines [had] been called into question," and several email exchanges had been leaked suggesting that employees knew about the machines' deficiencies.⁵⁸ The plaintiffs posted the leaked emails online, and an online newspaper outlet published an article that criticized Diebold and linked to the emails posted by the plaintiffs.⁵⁹ Diebold then sent DMCA takedown requests to the ISPs hosting the leaked emails "in an alleged effort to prevent further public viewing of the email archive."⁶⁰ Even though Diebold did not thereafter sue the plaintiffs for copyright infringement, the plaintiffs sued Diebold for violation of § 512(f) of the DMCA.⁶¹

The case, which was decided in 2004, held that the copyright holder violated § 512(f) by "knowingly materially misrepresent[ing]" that the plaintiffs had violated their copyright.⁶² In reaching this decision, the court emphasized that "[t]he fact that Diebold never actually brought suit against any alleged infringer suggests

54. 17 U.S.C. §§ 512(f)(1)–(2) (2010).

55. 337 F. Supp. 2d 1195 (N.D. Cal. 2004).

56. *Id.*

57. *Id.* at 1198–99.

58. *Id.* at 1197.

59. *Id.* at 1197–98.

60. *Id.* at 1198.

61. *Id.* at 1199.

62. *Id.* at 1204.

strongly that Diebold sought to use the DMCA's safe harbor provisions—which were designed to protect ISPs, not copyright holders—as a sword to suppress publication of embarrassing content rather than as a shield to protect its intellectual property.”⁶³ Using a takedown request as a sword—that is, using it as an affirmative means of accomplishing a strategic end, rather than as a defensive measure to protect one's copyright—is thus an impermissible use of the notice-and-takedown structure and is actionable under § 512(f).

Recognizing that this was a case of first impression, the court defined “knowingly materially misrepresents” as follows:

A party is liable if it “knowingly” and “materially” misrepresents that copyright infringement has occurred. “Knowingly” means that a party actually knew, should have known if it acted with reasonable care or diligence, or would have had no substantial doubt had it been acting in good faith, that it was making misrepresentations. “Material” means that the misrepresentation affected the ISP's response to a DMCA letter.⁶⁴

Here, because “[n]o reasonable copyright holder could have believed that the portions of the email archive discussing possible problems with Diebold's voting machines” were an infringement of Diebold's copyright under the circumstances, and because it was clear that Diebold knew that the takedown requests would result in online removal of the email content, Diebold was liable under § 512(f).⁶⁵

2. *Rossi*

Rossi v. Motion Picture Association of America Inc. was decided just a few months after *Diebold*, and addressed the “good faith belief” requirement of § 512(c) of the DMCA.⁶⁶ *Rossi* reconciled the “good faith belief” standard of section 512(c) with the “knowing misrepresentation” standard of § 512(f), finding that liability can only be imposed for a “knowing misrepresentation” under § 512(f).⁶⁷

In this case, the plaintiff was the owner and operator of a website that “provided visitors with a directory of websites containing information about movies.”⁶⁸ A Motion Picture Association of American (“MPAA”) member alerted the MPAA to the plaintiff's website, which the MPAA then examined and found to include text suggesting the availability of pirated film content.⁶⁹ Even though the MPAA found content on the plaintiff's website suggesting film piracy, “[i]t is undisputed that MPAA did not attempt to download any movies from [the plaintiff's] website or

63. *Id.* at 1204–05.

64. *Id.* at 1204 (internal citations omitted).

65. *Id.* at 1204.

66. 391 F.3d 1000 (9th Cir. 2004).

67. *Id.* at 1004–05.

68. *Id.* at 1001–02.

69. “A subsequent examination of Rossi's website revealed the following contents: ‘Join to download full length movies online now! new movies every month’; ‘Full Length Downloadable Movies’; and ‘NOW DOWNLOADABLE.’” *Id.* at 1002.

any links to the site.”⁷⁰ The MPAA sent a takedown request to the ISP hosting the plaintiff’s website, and within a few days, the plaintiff found a new ISP to host his website.⁷¹ The plaintiff sued the MPAA under several tort causes of action, asserting that the MPAA had not complied with § 512(c)’s “good faith belief” requirement in sending its takedown notices.⁷²

In finding for the MPAA, the court held that the “good faith belief” requirement in § 512(c) “encompasses a subjective, rather than objective, standard.”⁷³ Comparing the § 512(c) “good faith” standard with the “knowing misrepresentation” standard of § 512(f), the court held that “[a] copyright owner cannot be liable simple because an unknowing mistake is made,” but “[r]ather, there must be a demonstration of some *actual knowledge of misrepresentation* on the part of the copyright owner.”⁷⁴ The court found that the MPAA met this standard when it investigated the plaintiff’s website and found statements that suggested piracy of the MPAA’s copyrighted films.⁷⁵

3. *Lenz*

Lenz v. Universal Music Corp.,⁷⁶ decided in 2008 and affirmed by the Ninth Circuit in 2015,⁷⁷ applied the *Diebold* and *Rossi* standards of liability to a robot-takedown request and further defined the contours of a § 512(f) claim. In *Lenz*, an individual user posted a video of her son on YouTube in which the child danced to the artist Prince’s song “Let’s Go Crazy” which was playing audibly in the background.⁷⁸ Universal Music, which owns the copyright to the song, sent a takedown request to YouTube demanding that the song be removed, after which YouTube removed the video from its site.⁷⁹ *Lenz* followed the counter-notification procedure, and six weeks later, YouTube reinstated the video.⁸⁰ *Lenz* then sued Universal for misuse of the takedown procedure under § 512(f).⁸¹

The district court tackled the issue of whether *Diebold* and *Rossi* required a copyright holder to consider the possible applicability of fair use before sending a takedown request.⁸² The court held that “in order for a copyright owner to proceed under the DMCA with a good faith belief that use of the material in the manner

70. *Id.* at 1003.

71. *Id.* at 1002.

72. *Id.* at 1002–03.

73. *Id.* at 1004.

74. *Id.* at 1005 (emphasis added).

75. “As the district court noted, there is little question that these statements strongly suggest, if not expressly state, that movies were available for downloading from the site.” *Id.* at 1005 (internal quotations omitted).

76. 572 F. Supp. 2d 1150 (N.D. Cal. 2008) (“*Lenz I*”).

77. *Lenz v. Universal Music Corp.*, 801 F.3d 1126 (9th Cir. 2015) (“*Lenz II*”).

78. *Lenz I*, 572 F. Supp. 2d at 1151–52.

79. *Id.* at 1152.

80. *Id.*

81. *Id.* at 1153.

82. *Id.* at 1154–55.

complained of is not authorized by the copyright owner, its agent, or the law, the owner must evaluate whether the material makes fair use of the copyright.”⁸³ Thus, “[a]n allegation that a copyright owner acted in bad faith by issuing a takedown notice without proper consideration of the fair use doctrine . . . is sufficient to state a misrepresentation claim pursuant to Section 512(f) of the DMCA.”⁸⁴ Applying *Rossi*, the court held that while a copyright owner must consider fair use as part of its initial review of a potential infringement, it need not conduct “a full investigation.”⁸⁵

Interestingly, the Ninth Circuit opinion affirming the district court holding specifically mentioned the potential use of automated takedown processes, albeit in dicta. The court stated: “We note, without passing judgment, that the implementation of computer algorithms appears to be a valid and good faith middle ground for processing a plethora of content while still meeting the DMCA’s requirements to somehow consider fair use.”⁸⁶ Thus, the Ninth Circuit seemed to be adopting the view that the use of automated processes on its face does not violate § 512(f).

II. THE PROBLEMATIC NOTICE-AND-TAKEDOWN ENVIRONMENT OF TODAY

A. DEFINING THE “PROBLEM” OF ROBO-TAKEDOWNS

This Note argues that robo-takedowns in and of themselves are not the problem—in fact, they are arguably the best means available for copyright holders to fight rampant piracy online, including the ever-present “whack-a-mole” problem.⁸⁷ Automated processes could also be the most efficient way for ISPs to deal with the increasingly high volume of takedown requests they receive.⁸⁸ But, with the rise of automated takedown regimes, there is an increased risk that robo-takedown requests will result in the erroneous takedown of noninfringing content,

83. *Id.* (citing 17 U.S.C. § 512(c)(3)(A)(V)) (internal quotations omitted).

84. *Id.*

85. *Id.* at 1156.

86. *Lenz II*, 801 F.3d 1126, 1135. The court went on to say that “consideration of fair use may be sufficient if copyright holders utilize computer programs that automatically identify for takedown notifications content where: ‘(1) the video track matches the video track of a copyrighted work submitted by a content owner; (2) the audio track matches the audio track of that same copyrighted work; and (3) nearly the entirety . . . is comprised of a single copyrighted work.’” *Id.*

87. See, e.g., Daniel Seng, *The State of the Discordant Union: An Empirical Analysis of the State of DMCA Takedown Notices*, 18 VA. J.L. & TECH. 369, 376 (2014) (“[T]he takedown process . . . is the mainstay of content providers for managing online infringement because it is fast, cheap, and efficient.”).

88. At least one federal judge agrees with this proposition. See *Perfect 10, Inc. v. Giganews, Inc.*, No. 11-CV-07098-AB (SHx), 2015 WL 1746406, at *10 (C.D. Cal. Mar. 6, 2015) (“[Defendant’s] automated system is essential to expeditiously processing takedown notices in light of the staggering volume of requests Giganews receives—in the year between November 6, 2012 and November 6, 2013, Giganews processed more than half-a-billion takedown notices.”).

resulting in a chilling effect on free speech.⁸⁹ This is largely due to takedown requests that are overly broad—i.e., requests that, in an attempt to target legitimately infringing content, also target content that somehow appears to be infringing but in fact is not.

Next, there appears to be a relatively low incidence of user pushback on takedown requests.⁹⁰ This could mean two things: either the user pushback mechanism is flawed and users do not push back when they actually have legitimate claims, or users are pushing back when they have legitimate claims and the incidence of overly broad requests is actually relatively low (meaning that robot-takedown regimes are, in fact, operating effectively). This Note does not attempt to fully answer the question of why there is a low incidence of user pushback on takedown requests, but rather aims to provide additional data that can hopefully be useful in this inquiry.

1. Overbroad Takedown Requests

A potential response to the aforementioned “whack-a-mole” problem is to use automated processes to send frequent—and voluminous—requests to ISPs in the hope that a steady stream of takedown requests will target any infringing content that continues to reappear. While copyright holders are generally hesitant to admit to this strategy, evidence suggests that ISPs are currently saddled with a steady stream of requests that is both increasing⁹¹ and high in volume.⁹² The ISPs themselves face limited resources and the ever-present risk of losing safe harbor protection if they fail to “expeditiously” remove content pursuant to takedown requests.⁹³ This environment incentivizes the issuance of overbroad requests at the expense of individual users without much recourse for the copyright holders, thus creating a perfect storm for the chilling of free speech.⁹⁴

Determining the exact number or proportion of overbroad requests is currently impossible, as information regarding the number of takedown requests actually

89. See Seltzer, *supra* note 15.

90. See *infra* Part II.A.2.

91. Google reports that the number of requests they receive “has been increasing rapidly.” Fred von Lohmann, *Transparency for copyright removals in search*, GOOGLE OFFICIAL BLOG (May 24, 2012), <http://googleblog.blogspot.com/2012/05/transparency-for-copyright-removals-in.html>.

92. In 2014 alone, Google received requests for more than 345 million allegedly-infringing links. Ernesto Van der Sar, *Google Asked to Remove 345 Million ‘Pirate’ Links in 2014*, TORRENTFREAK (Jan. 5, 2014), http://torrentfreak.com/google-asked-remove-345-million-pirate-links-2014-150105/?utm_source=dlvr.it&utm_medium=twitter [https://perma.cc/FD8U-ZFH6].

93. 17 U.S.C. § 512(c)(1)(A)(iii).

94. “[T]he effect of the DMCA’s takedown provisions has been to allow the copyright owners to escape any burden. The copyright owners send takedown notifications attesting good-faith belief, and the ISPs promptly remove the offending material. If the Internet users sue, they must prove bad faith.” Benjamin Wilson, Comment, *Notice, Takedown, and the Good-Faith Standard: How To Protect Internet Users from Bad-Faith Removal of Web Content*, 29 ST. LOUIS U. PUB. L. REV. 613, 636 (2010) (internal citations omitted); see also Seltzer, *supra* note 15, at 178 (arguing that “the DMCA is systematically susceptible to abusive claims”).

issued is limited.

But, there is at least some evidence of overbroad robo-takedown requests. In 2012, Google reported that they refused to comply with around 3% of the DMCA takedown requests they received for Google Search, at least some of which were overbroad.⁹⁵ The Electronic Frontier Foundation (“EFF”) went further, sifting through the data in Google’s 2012 Transparency Report and finding additional instances of seemingly overbroad takedown requests.⁹⁶ The EFF also created an online “Hall of Shame” to highlight instances of “particularly bogus takedowns” based on anecdotal evidence from people who claim to have received takedown notices from a variety of ISPs.⁹⁷ Website TorrentFreak also highlights overbroad requests on its site each week, using data from a DMCA takedown clearing house.⁹⁸ Thus, even though the data on overbroad takedown requests is not fully determinative, there is at least some evidence to suggest that overbroad requests do occur and result in the takedown of noninfringing content.

2. Lack of User Pushback

Based on studies conducted by Congress and the Center for the Protection of Intellectual Property, as well as self-reported anecdotal evidence compiled by copyright holders and Internet watchdogs alike, there appears to be a very low incidence of user pushback generally.⁹⁹ Assuming this to be true, the reason for the low pushback remains unclear. A lack of user pushback could mean a lot of things, including that the counter-notification procedure may be too arduous or intimidating for users to pursue.¹⁰⁰ Indeed, § 512(g)’s requirement that users

95. See, e.g., Google, *Google Transparency Report FAQ*, https://www.google.com/transparencyreport/removals/copyright/faq/#compliance_rate [<https://perma.cc/4LKJ-2R9P>] (last visited Jan. 14, 2015).

96. Parker Higgins & Kurt Opsahl, *Top 10 Takedowns in Google’s Copyright Transparency Report*, ELEC. FRONTIER FOUND. (July 5, 2012), <https://www.eff.org/deeplinks/2012/07/top-10-takedowns-googles-copyright-transparency-report> [<https://perma.cc/UQ6F-FRL9>].

97. ‘Hall of Shame’ Calls Out Bogus Internet Censorship, ELEC. FRONTIER FOUND. (Oct. 27, 2009), <https://www.eff.org/press/archives/2009/10/27> [<https://perma.cc/EPY2-FPXQ>].

98. See, e.g., Ernesto Van der Sar, *MPAA Targets Reddit Community Over Movie Piracy*, TORRENTFREAK (June 24, 2014), <https://torrentfreak.com/mpaa-targets-reddit-movie-piracy-140624/> [<https://perma.cc/2RGF-UPSG>].

99. See, e.g., *Section 512 of Title 17: Hearing Before the Subcomm. on Courts, Intellectual Property, and the Internet of the Comm. on the Judiciary*, 113th Cong. 59 (2014) (statement of Paul Sieminski, General Counsel for Automattic Inc.) [hereinafter *Hearing*]; Bruce Boyden, *The Failure of the DMCA Notice and Takedown System: A Twentieth Century Solution to a Twenty-First Century Problem*, CENTER FOR THE PROTECTION OF INTELLECTUAL PROPERTY 3 (2013), <http://cpip.gmu.edu/wp-content/uploads/2013/08/Bruce-Boyden-The-Failure-of-the-DMCA-Notice-and-Takedown-System1.pdf>; Motion Picture Association of America, *Comments on Department of Commerce Green Paper, Copyright Policy, Creativity, and Innovation in the Digital Economy*, No. 130927852-3852-01, at 4 (Nat’l Telecomm. & Info. Admin. Nov. 13, 2013), https://www.ntia.doc.gov/files/ntia/motion_picture_association_of_america_comments.pdf (stating that the MPAA received eight counter-notifications for a period of a few months in 2013).

100. This is especially likely considering the DMCA’s requirement that the user submit to the court’s jurisdiction to employ the counter-notification procedure. See *supra* Part I.A.3.

submit to the jurisdiction of the courts before they can counter-notify has resulted in at least some instances in which users provide false information in their counter-notification.¹⁰¹ The expense of litigating a suit could also deter users from seeking relief from the courts, even where the user believes she has a strong case.¹⁰² Further, users could simply be confused about the recourse options available to them.¹⁰³ Conversely, the lack of user pushback could mean that much of the content removed pursuant to takedown requests is, in fact, infringing.¹⁰⁴

While the reason for lack of user pushback is unclear, there is a structural aspect of the notice-and-takedown system that provides cause for concern. In the non-digital world, when an individual receives a cease and desist letter for a non-digital work (a painting, for example) alleging that the work infringes someone's copyright, the individual is able to contest the letter while her work remains undisturbed. In the digital world, by contrast, takedown requests result in the removal of content as a first step, with any dispute over the fact of infringement occurring later.¹⁰⁵ This creates the potential for chilling effects on free speech in the digital world only, with the notice-and-takedown mechanism serving as a form of preemptive censorship. As a purely structural matter, therefore, the need for a strong user-notification procedure is imperative.

B. DETERMINING THE SCOPE OF THE PROBLEM

Only a few empirical studies have been conducted thus far that thoroughly parse the data currently available on takedown requests. While no one study provides a fully comprehensive snapshot of the takedown environment today, each provides valuable insight into the nature of the requests being issued.

101. See, e.g., *Crunchyroll, Inc. v. Pledge*, C 11-2334 SBA, 2014 WL 1347492, at *7 (N.D. Cal. Mar. 31, 2014).

102. Oftentimes, an individual user with limited resources would be going up against a large company with the vast resources to effectively litigate a case, which makes it even more unlikely that the user would choose to sue. See *Hearing*, *supra* note 99, at 64 (statement of Mr. Paul Sieminski, General Counsel for Automattic Inc.).

103. For example, information posted by ISPs about their counter-notification procedure does not always answer all of a user's questions, and different ISPs have varying policies as to how they treat counter-notifications. See Parker Higgins, Corynne McSherry, & Daniel Nazer, *Who Has Your Back? Protecting Your Speech from Copyright & Trademark Bullies*, ELEC. FRONTIER FOUND. 7–8 (2014), https://www.eff.org/files/2014/10/27/who-has-your-back-2014-copyright-trademark_0.pdf (“For example, while Pinterest’s terms outline a counter-notice procedure, they do not commit to restoring content if the person who filed the original complaint does not file a lawsuit. Similarly, Tumblr only says it ‘may restore’ counter-noticed works. By contrast, Facebook’s policy clearly provides the necessary information.”).

104. A low incidence of user pushback could simply mean that § 512 is working as intended. See, e.g., Jennifer M. Urban & Laura Quilter, *Efficient Process or “Chilling Effects”?: Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH L.J. 621, 631 (2006) (“[T]he vast majority of 512 notices likely are never subject to the scrutiny of a court. In part, this was precisely the point behind 512: the efficient removal of infringing materials from the Internet in a fair process, with (in most cases) no need for court review.”).

105. See *supra* notes 91–98.

It is important to note upfront some of the limiting factors affecting any analysis of the data currently available on takedown requests and counter notifications, including the findings presented in section II.C. of this Note. First and perhaps most importantly, the data currently available is incomplete and thus it is impossible for any analysis to be fully comprehensive. The major ISPs do not currently release all possible data related to the takedown requests or counter-notifications they receive, nor are they required to do so by the DMCA.¹⁰⁶ Second, since the DMCA does not include a reporting requirement, all data collected by any organization of its own volition is subject to potential institutional biases and should be regarded with the appropriate amount of caution.

Many ISPs began releasing data only after Google released its first Transparency Report in 2009, and much of this data is limited.¹⁰⁷ Google, for example, only releases data about a few of its products, and only after a certain date.¹⁰⁸ YouTube employs a Content ID system that falls outside the ambit of § 512 and accounts for the majority of takedown requests YouTube receives.¹⁰⁹ This limits all analysis of takedown requests received by Google to Google's non-YouTube § 512(c) UGC websites, like Blogger and Google Play, and amplifies the proportion of requests received pursuant to § 512(d), which reflects information location tools like Google Search. This is a major limiting factor, as it does not account for the proportion of the notice-and-takedown landscape that is undoubtedly dominated by YouTube.

Aside from ISPs, a few notable organizations have been trying to compile data on takedowns and counter-notifications. Harvard Law School started an online repository of such self-reported requests, Chilling Effects—since renamed Lumen¹¹⁰—which was and continues to be perhaps the largest repository currently available.¹¹¹ Chilling Effects and Lumen have proven to be a valuable resource for researchers, and several ISPs, including Google and Twitter, automatically send

106. See Seng, *supra* note 87, at 378.

107. See Betsey Isaacson, *55 Charts That Prove Governments Are Increasingly Censoring Your Internet*, HUFFINGTON POST (July 3, 2013, 1:01 PM), http://www.huffingtonpost.com/2013/07/03/government-censor-internet_n_3535322.html [<https://perma.cc/SHM8-YJSW>].

108. In particular, Google did not start releasing information regarding DMCA takedown requests until 2012. See GOOGLE OFFICIAL BLOG, *supra* note 91.

109. Seng, *supra* note 87, at 386.

110. The Chilling Effects website now now redirects to the Lumen site. See CHILLING EFFECTS, <https://www.chillingeffects.org/pages/about> (last visited Jan. 14, 2015); *About Us*, LUMEN, <https://lumendatabase.org/pages/about> [<https://perma.cc/S2GA-CQUG>] (last visited Apr. 4, 2016). Lumen's blog describes the creation of the Lumen site, and the migration of the Chilling Effects database to the new site, as resulting from the "astonishing growth" of the Chilling Effects database; Lumen reports that in October 2015, Chilling Effects received its one billionth allegedly-infringing URL. *Blog*, LUMEN (Nov. 2, 2015), https://lumendatabase.org/blog_entries/763 [<https://perma.cc/33CL-DA9C>].

111. Due to pressure from copyright holders unhappy with Chilling Effects' collection of non-linked infringing websites, Chilling Effects decided to remove its site from major search engines in January 2015. Ernesto Van der Sar, *Chilling Effects DMCA Archive Sensors Itself*, TORRENTFREAK (Jan. 10, 2015), <https://torrentfreak.com/chilling-effects-dmca-archive-censors-itself-150110/> [<https://perma.cc/M3QA-QBX9>].

takedown notices to its repository.¹¹² The EFF also collects self-reported takedown data, though not in as comprehensive a fashion as Chilling Effects or Lumen.

1. Urban and Quilter Study

A seminal study conducted in 2006 by Jennifer Urban and Laura Quilter marked the first time researchers attempted to compile empirical data on takedown regimes and it remains a valuable resource today in tracking the evolution of the notice-and-takedown system over time.¹¹³ The researchers used a coding procedure to analyze nearly 900 takedown requests collected from a variety of sources, including those that had been submitted to Google and Chilling Effects, in an attempt to ascertain the number of takedown requests that result in the removal of legitimate, noninfringing content.¹¹⁴ The study found that while corporate entities sent the majority of § 512(c) takedown requests,¹¹⁵ requests sent by the movie and music industries only comprised 6% of the total requests issued.¹¹⁶ Together, the Recording Industry of America (“RIAA”) and the MPAA sent only nine notices under §§ 512(c) and 512(d).¹¹⁷ Even more surprisingly, the data revealed that 41% of all requests submitted to Google targeted “competitors of the complainants,” while 21% of §§ 512(c) and 512(d) notices sent to Google “target[ed] hobbyists, critics and educational users.”¹¹⁸ Next, turning to the content of the takedown requests themselves, the researchers concluded that a shocking 31% of §§ 512(c) and 512(d) notices raised issues “related to the underlying copyright claim, including fair use defenses, other substantive defenses, very thin copyright, or non-copyrightable subject matter.”¹¹⁹ As to the incidence of counter-notification, the study found only seven counter-notices in the entire dataset.¹²⁰ It is important to note, however, that this small number could be due to the relatively low incidence of § 512(c) notices at the time, because only § 512(c) obligates ISPs to inform takedown recipients of the counter-notification procedure. Lastly, the study also concluded that § 512(c) notices were on the rise, even back in 2006.¹²¹

This study provides meaningful insight into the way takedown requests are used, but is limited in a number of ways. As an initial matter, the study was conducted before the rise in popularity of such UGC sites as YouTube and Twitter, and thus the majority of the takedown requests studied were actually submitted pursuant to § 512(d) and not § 512(c).¹²² We can thus expect that a study conducted today using

112. Seng, *supra* note 87, at 381–82, n.37 and n.43.

113. Urban & Quilter, *supra* note 104.

114. Urban & Quilter, *supra* note 104, at 623.

115. Urban & Quilter, *supra* note 104, at 649–50.

116. Urban & Quilter, *supra* note 104, at 651.

117. Urban & Quilter, *supra* note 104, at 655.

118. Urban & Quilter, *supra* note 104, at 655.

119. Urban & Quilter, *supra* note 104, at 667.

120. Urban & Quilter, *supra* note 104, at 679.

121. Urban & Quilter, *supra* note 104, at 645–46.

122. In fact, only 315 § 512(c) notices, and sixty-eight “§ 512(c)-like notices,” were available for

a similar methodology might lead to much different results.¹²³ Next, the sample size is relatively small—in 2006, not many takedown requests were issued at all and robo-takedown regimes had not yet become prevalent—and Google notices comprised a large majority of the data set.¹²⁴ Lastly, the industry-specific results no longer seem to be entirely relevant; today, the entertainment industries overwhelmingly send the most takedown requests according to Google’s Copyright Transparency Report.¹²⁵

2. Seng Study

A more recent study conducted by Daniel Seng provides additional and fascinating insight into the state of takedown regimes today, including the rise of robo-takedown regimes in particular.¹²⁶ Similar to the Urban and Quilter study, this study performs an empirical analysis of the notice-and-takedown landscape using data from the Chilling Effects repository. In contrast to the Urban and Quilter study, however, the Seng study does not attempt to analyze the content of the requests themselves, but rather tracks the number of requests issued and analyzes the quantitative data in various ways.¹²⁷

Amazingly, Seng analyzed half-a-million takedown notices and over 50 million takedown requests in total,¹²⁸ beginning with those first submitted to Chilling Effects and ending with those submitted December 31, 2012.¹²⁹ In order to tackle the vast amount of data contained within the half-a-million takedown notices, Seng developed algorithms to parse the data and extracted thirty-six fields, resulting in over 50 million individual requests.¹³⁰ Seng then analyzed these two datasets independently, drawing a variety of interesting and illuminating conclusions. First, as to the identity of the copyright holders sending takedown requests, Seng found that the top twenty most frequent issuers of takedown notices comprise companies and organizations from the music, movie, adult entertainment, book, and software

study. Urban & Quilter, *supra* note 104, at 644.

123. For example, the Takedown Project, discussed *infra* Part II.B.3, promises to yield fascinating results.

124. Urban & Quilter, *supra* note 104, at 642.

125. GOOGLE TRANSPARENCY REPORT, <http://www.google.com/transparencyreport/removals/copyright/owners/?r=all-time> [<https://perma.cc/WJ7T-QNSN>] (last visited Jan. 13, 2015).

126. Seng, *supra* note 87.

127. Among the questions the Seng study seeks to answer: “Who are the copyright owners that use takedown notices? Who are the reporters serving the takedown notices on service providers? Are there different types of reporters? Who are the intermediaries who, as service providers, are served with the notices? Are there different types of notices? And which safe harbor provisions in the DMCA are addressed in these takedown notices and requests?” Seng, *supra* note 87, at 376.

128. Seng distinguished between takedown notices and takedown requests in his study. As defined in the study, a “notice” is the document that the copyright holder sends to the ISP requesting takedown of allegedly infringing material, and a “request” is the individual identification of allegedly-infringing content. Thus, a “notice” can contain several individual “requests.” See Seng, *supra* note 87, at 375-76 nn.18–19.

129. Seng, *supra* note 87, at 382.

130. Seng, *supra* note 87, at 381–82.

industries, with 68.1% sent by the music and movie industries alone.¹³¹ As to the incidence of counter-notification, Seng found that while no counter-notices were served between 2008 and 2010, they comprised 0.131% of all notices in 2011 and 0.020% of all notices in 2012.¹³² In total, there were fifty-nine counter-notices issued pursuant to § 512(c) in 2011, and eighty-two in 2012.¹³³ This data presents a significant increase from the seven counter-notices found by Urban and Quilter in 2006, but still shows that counter-notifications represent a markedly low proportion of the total number of notices sent each year.

Interestingly, Seng was able to analyze an automated removal procedure implemented by Google for which little public information is available. Seng describes Google's Trusted Copyright Removal Program ("TCRP") as "an automated method for providers and agents to submit large numbers of notices and takedown requests electronically to Google, which Google would process rapidly via an automated process."¹³⁴ By searching the Chilling Effects repository for the electronic "Trusted User" signatures of TRCP participants, Seng was able to look at data that he believes is representative of the TRCP program.¹³⁵ The data suggests that the participants are largely well known copyright holder companies, many of whom are also known to send high volumes of takedown notices, like the RIAA and BPI.¹³⁶ The data also reveals that the program has resulted in Google's receipt of 376 thousand notices and 54 million takedown requests, with an overall compliance rate of 96.2%.¹³⁷ Even though not much is currently known about this program, and although it falls outside the ambit of § 512, it could potentially serve as an interesting model for creating more effective automated takedown procedures to combat piracy.

The Seng study acknowledges a variety of limitations that are similar to those faced by the Urban and Quilter study. For one, the data is limited to what is available through the Chilling Effects repository, and a large percentage of the requests are from Google.¹³⁸ Secondly, because Google does not make data from its YouTube Content ID system publicly available through Chilling Effects or otherwise, the Seng study does not include any of this information in its analysis.¹³⁹ Google began reporting YouTube takedown requests in 2012, but that data is severely limited and likely not indicative of the volume of requests YouTube receives each year. Thus, similar to the limitation encountered in the Urban and Quilter study, the Seng study is largely representative of takedown notices submitted pursuant to § 512(d) as opposed to § 512(c). While this was not a

131. Seng, *supra* note 87, at 393–94.

132. Seng, *supra* note 87, at 462.

133. Seng, *supra* note 87, at 428.

134. Seng, *supra* note 87, at 414.

135. Seng, *supra* note 87, at 415.

136. Seng, *supra* note 87, at 457.

137. Seng, *supra* note 87, at 415–17.

138. Seng, *supra* note 87, at 384.

139. Seng, *supra* note 87, at 386–87.

particularly limiting factor in the Urban and Quilter study for the obvious reason that YouTube did not exist at the time the analysis was conducted, it does present a major limiting factor in the Seng study's ability to provide a comprehensive snapshot of the takedown environment, as annual YouTube takedowns are believed to number in the millions.¹⁴⁰ But, until Google makes this information publicly available, its absence will remain an unavoidable limitation for any current and future research.

3. The Takedown Project

The Takedown Project, a collaboration between researchers from Berkeley Law School and the American Assembly at Columbia University, is currently performing studies that seek to expand upon the work conducted in the Urban and Quilter study with more recent data and a much broader data set.¹⁴¹ One of the projects, the Notice Coding Engine, utilizes both manual and machine coding to analyze the effect of automated processes on the notice-and-takedown procedure.¹⁴² The other project, the Notice and Takedown Survey, will add to this information by conducting surveys of both large and small online service providers to learn about their experiences with and thoughts on the notice-and-takedown system.¹⁴³ While the results from this project are forthcoming, it promises to provide valuable information on the notice-and-takedown landscape.¹⁴⁴

4. The NYU Counter-Notification Study

NYU School of Law's Brennan Center for Justice issued a report in 2005 in which researchers followed up with the recipients of takedown notices "to learn

140. Seng, *supra* note 87, at 386-87.

141. TAKEDOWN PROJECT, <http://takedownproject.org/projects> [https://perma.cc/A6XJ-5XNH] (last visited Feb. 20, 2016).

142. *Id.*

143. *Id.*

144. In 2015, one of the Takedown Project researchers gave a presentation at the 10th Annual European Policy for Intellectual Property Conference entitled, "Notice and Takedown in the Age of the Robo Notice." The abstract for the presentation describes the Takedown Project's research inquiry as follows:

The practice of notice and takedown under the DMCA has changed dramatically in the last five or six years, driven by the adoption of automated notice-sending systems. As these systems became common, the number of takedown requests to many services skyrocketed, quickly overwhelming human vetting at the targeted services. Increasingly, the online regulation of speech passes through such systems, subject to little human intervention or verification and a relatively poor record of accuracy. Our work traces this history and evaluates the reliability of automated procedures, based on interviews with service providers and coding of Google Search notices.

Joe Karaganis, EUROPEAN POLICY FOR INTELLECTUAL PROPERTY 10TH ANNUAL CONFERENCE, <http://www.epip2015.org/notice-and-takedown-in-the-age-of-the-robo-notice/> [https://perma.cc/8GPG-8LEW] (last visited Feb. 20, 2016). The results of this research promise to be particularly pertinent to the subject of this Note.

how well fair use and free expression are faring among artists, scholars, and others who make critical contributions to culture and democratic discourse.”¹⁴⁵ The researchers analyzed 320 cease and desist letters and takedown notices from Chilling Effects, conducted telephone interviews with seventeen recipients of takedown notices, and compiled the responses of 290 individuals who filled out an online survey about copyright and fair use.¹⁴⁶ The study concluded that of the seventeen individuals interviewed on the telephone, five had “strong or at least reasonable fair use or First Amendment defenses,” “four had possible defenses,” and seven received notices “with weak copyright and trademark claims,” but nine of the seventeen “acquiesced in the copyright or trademark owners’ demands, or had their material removed because of take-down letters.”¹⁴⁷

C. EMPIRICAL ANALYSIS OF LITIGATION ARISING FROM POTENTIAL MISUSE OF THE NOTICE-AND-TAKEDOWN PROCEDURE

While there are many important studies analyzing the current notice-and-takedown environment, there are currently no studies that look specifically at the litigation arising from possible misuses of the takedown procedure. In order to attempt to fill this gap, this Note looks at the possibility of takedown abuse by attempting to identify and analyze all post-*Diebold* litigation arising from user pushback on takedown requests issued by copyright holders under § 512(c).¹⁴⁸ While an attempt was made to identify cases involving use of a robo-takedown, the research was not limited to cases arising from use of such requests.¹⁴⁹

I chose to focus on litigation rather than the data available on takedown requests or counter notifications themselves both because data regarding these requests is not readily available and because, of the data that is available, more resources than I have at my disposal would be required to parse through the data in a meaningful way. Also, important analysis of this data is already currently underway and promises to yield interesting and illuminating results.¹⁵⁰ My research also does not attempt to capture the incidence of counter-notification generally for similar reasons. Further, by analyzing litigation as opposed to the takedown requests or counter notifications themselves, I was able to focus my research on the potential misuse of takedown requests issued pursuant to § 512(c) as opposed to § 512(d). I felt that focusing on § 512(c) would be more representative of the overall state of notice-and-takedown practices, as much of the controversy regarding abuse of the

145. MARJORIE HEINS & TRICIA BECKLES, BRENNAN CENTER FOR JUSTICE, WILL FAIR USE SURVIVE? FREE EXPRESSION IN THE AGE OF COPYRIGHT CONTROL ii (2005).

146. *Id.*

147. *Id.*

148. Findings were intentionally limited to cases involving individual users and copyright holders to keep the research scope to a manageable size. Instances of litigation arising from disputes between a copyright holder and an ISP, or a user and an ISP, were therefore excluded.

149. Indeed, it may even be impossible to distinguish the cases in such a way. Since automated notice-and-takedown systems are relatively new, court opinions do not always identify them as such.

150. *See supra* Part II.B.

takedown procedure centers on content uploaded to UGC sites. It is hoped that these findings, despite their limitations, may be useful in painting a picture of the larger notice-and-takedown landscape.

1. Limitations

Some inherent limitations to these findings should be noted. For one, even though the results that follow arise from extensive research using a variety of search parameters and both quantitative and qualitative data analysis, there is a possibility that some cases were simply missed in the research process. This can be attributed to the inherent limitations of my research methodology, particularly since reliance on search parameters to identify relevant cases requires that courts actually use those terms in their opinions, and that the relevant cases are actually located.

Next, the data's usefulness in analyzing the effectiveness of the counter-notification procedure—or the incidence of counter-notification generally—is limited. It is often hard to tell in the text of the cases themselves when the counter-notification procedure was or was not followed. Thus, the data on the incidence of counter-notification below only reflects instances in which the counter-notification procedure was explicitly mentioned in the court opinion. In the future, it would be helpful for courts to specifically mention use of the counter-notification procedure where it is employed so that research into this area can be more effective, comprehensive, and, ultimately, more useful.

2. Methodology

The research was conducted using a variety of search parameters to identify relevant cases on Westlaw.¹⁵¹ Once relevant cases were identified, they were read to ensure relevancy and then relevant information from each case was compiled. This part of the research was initially completed on January 3, 2015 and then revisited in February 2016 in preparation for the publication of this Note.

The cases were then broken down into categories based on the scenario in which the litigation arose. The analysis revealed three key scenarios that seemed most relevant in identifying situations where there may have been misuse of the notice-and-takedown procedure as between a user and a copyright holder. In all instances, a copyright holder first sent a DMCA takedown request to an ISP pursuant to § 512(c) requesting that the user's allegedly infringing content be removed, and the user was notified of the takedown. The categories were distinguished based on what followed.

In "category one" cases, the user issued a § 512(g) counter-notification, and the copyright holder decided to pursue her copyright infringement claim anyway, or the user filed a declaratory action on the issue of copyright infringement. The underlying claims were thus copyright infringement claims.

151. Complaints for which no opinion had yet been written were not included in the research.

In “category two” cases, the user issued a § 512(g) counter-notification, and the copyright holder decided not to pursue a copyright infringement claim, but the user thereafter decided to pursue a § 512(f) misrepresentation claim against the copyright holder. The underlying claims were thus § 512(f) claims. Category two also included situations in which the user did not issue a § 512(g) counter-notification but still pursued a § 512(f) misrepresentation claim against the copyright holder after receiving notice of the takedown.

Finally, in “category three” cases, one party asserted an infringement claim and the other asserted a § 512(f) claim. Category three included claims both arising from § 512(g) counter-notification and those where counter-notification did not occur.

3. Findings

In all, twenty-four cases were found, analyzed, and categorized. Four cases were predicated on infringement claims (category one), sixteen were predicated on § 512(f) claims (category two), and four involved both infringement and § 512(f) claims (category three).

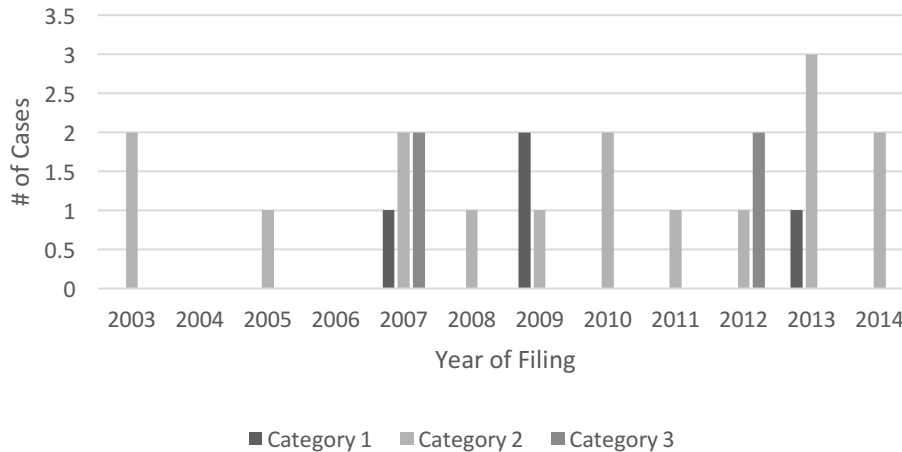


Figure 1. Year of Filing

The data reveals that, overall, the rate of claims stemming from takedown requests involving counter-notifications or potential § 512(f) violations has been fairly low since *Diebold*. It also shows that of all the types of cases that were studied, those involving § 512(f) claims where an underlying copyright dispute was not involved were the most prevalent, and those involving copyright infringement claims were the least prevalent. Thus, the type of case that appeared most frequently was that in which a user was the recipient of a takedown notice and

subsequently filed a § 512(f) claim, and where the copyright holder did not pursue a copyright infringement claim against the user. These cases included instances where the user employed the counter-notification procedure and where she did not, as well as cases where use of the counter-notification procedure was unclear. Notably, the incidence of these cases also appears to have remained the most stable over the time period examined. From 2003 to 2014 there was a steady stream of category two § 512(f) cases, whereas the number of category one and category three cases—both of which involve copyright infringement claims—exhibited more of an ebb and flow pattern. An interesting exception to the otherwise steady stream of § 512(f) cases is that there seems to have been a spike in the incidence of such cases in 2013. While the data alone is inconclusive as to the cause of the 2013 spike, it is possible that the upward trend will continue, particularly since two of the more recent cases studied both resulted in victories for the plaintiff.¹⁵²

Next, the scenario that occurred least frequently was that in which a takedown notice was issued and the copyright holder subsequently brought a copyright infringement claim. This includes both category one and category three cases, and therefore encapsulates instances where counter-notification may or may not have occurred.

Comparing the filing year findings to the Seng data, Seng found fifty-nine instances of counter-notifications arising from § 512(c) in 2011 and eighty-two in 2012.¹⁵³ Assuming the accuracy of all numbers under comparison, this would mean that in 2011, fifty-nine counter-notifications were issued, zero cases predicated on infringement alone were filed, one case predicated on § 512(f) was filed, and zero mixed infringement and § 512(f) cases were filed. In 2012, eighty-two counter-notifications were issued, zero infringement cases were filed, one § 512(f) case was filed, and two mixed infringement and § 512(f) cases were filed. This comparison reveals that the incidence of litigation in all categories compared to the incidence of counter-notifications is markedly low. While it's impossible to draw conclusions from this comparison, it does seem to suggest that, where the user chose to counter-notify, the copyright holder was unlikely to sue the user for copyright infringement. This could mean that the initial takedown requests in these scenarios were erroneous, or could simply mean that the copyright holder made a conscious decision not to pursue litigation for whatever reason. The comparison also suggests that where the user chose to counter-notify, the user was then almost equally unlikely to file a § 512(f) claim against the copyright holder. This could mean that the takedown requests in these scenarios were based on a good faith belief and the user recognized them as such, or that users in general do not yet fully understand their rights under § 512(f) and that an increase in future § 512(f) litigation is to be expected as the number of takedown requests—and, presumably, counter-notifications—increases.

152. See *infra* notes 159-60.

153. Seng, *supra* note 87, at 427-28.

a. *When a Copyright Holder Pursues an Infringement Claim (“Category One”)*

The table below demonstrates the number of pure copyright infringement claims arising from the counter-notification procedure.¹⁵⁴ There were four cases total, one of which was a declaratory action brought by the user. These cases were also fairly recent, with decisions reached in 2010, 2011, and 2012, and one case unresolved.

	<i>with counter- notification</i>	<i>total #</i>
<i>infringement claim fails</i>	0	0
<i>infringement claim succeeds</i>	3	3
<i>infringement claim unresolved</i>	1	1
		4

Figure 2. Category One Findings

One of the most interesting findings the research revealed was the incredibly low incidence of infringement claims occurring after a user’s counter-notification. This finding could demonstrate either that the notice-and-takedown system is working as intended, and that only users with colorable claims of noninfringement are counter-notifying; or, that the counter-notification procedure is underutilized, and that more users with colorable claims should feel empowered to counter-notify with the knowledge that not many of those counter-notifications give rise to litigation.

Also, the data shows that in instances where an infringement claim is waged after a user’s counter-notification, but where the user does not counterclaim with a § 512(f) claim (as in the category three cases), the infringement claim is more likely to succeed than it is to fail. This suggests that once a user pushes back on a takedown request by counter-notifying, copyright holders will only pursue litigation if they believe they have a strong case of copyright infringement. Where the copyright infringement case is weak, the copyright holder will not litigate the issue once a user pushes back. This is a logical result, but also presents a stark contrast between the number of counter-notifications that researchers believe are issued each year, as evidenced by the Seng data,¹⁵⁵ and the markedly low level of copyright infringement litigation that results from counter-notification, as

154. The cases were: *Vernor v. Autodesk, Inc.*, 621 F.3d 1102 (9th Cir. 2010); *Schenck v. Orosz*, No. 3:13-CV-0294, 2013 WL 5963557 (M.D. Tenn. Nov. 7, 2013); *Tetris Holding, LLC v. XIO Interactive, Inc.*, 863 F. Supp. 2d 394 (D. N.J. 2012); *Henley v. DeVore*, 733 F. Supp. 2d 1144 (C.D. Cal. 2010).

155. See *supra* Part II.B.2.

evidenced by this research. In order to issue a takedown request in the first place, a copyright holder must have a “good faith belief” that the material is infringing;¹⁵⁶ but if that’s the case, wouldn’t the copyright holder want to litigate the copyright infringement issue if the user pushes back? While definitive conclusions cannot be drawn from the data, the findings indeed suggest that at least some of the takedown requests issued each year are based on copyright claims that the copyright holder would choose not to defend in court following a user’s counter-notification.

b. When a User Asserts a Section 512(f) Misrepresentation Claim (“Category Two”)

The table below shows the number of pure § 512(f) claims that were uncovered in the research.¹⁵⁷ A total of sixteen cases were found.

	<i>with counter- notification</i>	<i>counter- notification unclear</i>	<i>total #</i>
<i>512(f) claim fails</i>	0	6	6
<i>512(f) claim succeeds</i>	2	1	3
<i>512(f) claim unresolved</i>	3	4	7
			16

Figure 3. Category Two Findings

156. 17 U.S.C. § 512(c)(3)(A)(v).

157. The cases were: *Handshoe v. Abel*, No. 1:14-CV-159-KS-MTP, 2016 WL 110519 (S.D. Miss. Jan. 8, 2016); *Automattic Inc. v. Steiner*, 82 F. Supp. 3d 1011 (N.D. Cal. 2015); *Curtis v. Shinsachi Pharm. Inc.*, 45 F. Supp. 3d 1190 (C.D. Cal. 2014); *Smith v. Summit Entm’t LLC*, No. 3:11-CV-348, 2011 WL 2200599 (N.D. Ohio June 6, 2011); *Flynn v. Siren-BookStrand, Inc.*, No. 4:13-CV-3160, 2013 WL 5315959 (D. Neb. Sept. 20, 2013); *Tuteur v. Crosley-Corcoran*, 961 F. Supp. 2d 333 (D. Mass. 2013); *Ouellette v. Viacom Int’l, Inc.*, No. CV 10-133-M-DWM-JCL, 2012 WL 1435703 (D. Mont. Apr. 25, 2012); *Does 1-4 v. Arnett*, No. SACV 12-96-JST, 2012 WL 3150934 (C.D. Cal. Aug. 1, 2012); *Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678 (D. Md. 2011); *Design Furnishings, Inc. v. Zen Path, LLC*, No. CIV 2:10-2765, 2010 WL 5418893 (E.D. Cal. Dec. 23, 2010); *Brave New Films 501(c)(4) v. Weiner*, 626 F. Supp. 2d 1013 (N.D. Cal. 2009); *Lenz v. Universal Music Corp.*, No. C 07-03783, 2008 WL 962102 (N.D. Cal. Apr. 8, 2008); *Doe v. Geller*, 533 F. Supp. 2d 996 (N.D. Cal. 2008); *Novotny v. Chapman*, No. 3:05-cv-370, 2006 WL 2335598 (W.D.N.C. Aug. 9, 2006); *Dudnikov v. MGA Entm’t, Inc.*, 410 F. Supp. 2d 1010 (D. Colo. 2005); *Online Policy Grp. v. Diebold*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004).

Notably, of the types of cases studied, pure § 512(f) claims far outnumbered those involving an underlying copyright infringement dispute. Also, a total of five cases include specific reference to use of the counter-notification procedure, and of these cases, two resulted in success on a § 512(f) claim and three remain unresolved. No case in which use of the counter-notification procedure was specifically mentioned in the court opinion resulted in a failed § 512(f) claim.

Still, six of the sixteen cases resulted in a failed § 512(f) claim. This could demonstrate the difficulty for a plaintiff to succeed on a § 512(f) theory, a phenomenon that has been documented and critiqued by researchers.¹⁵⁸ Interestingly, however, two of the three cases in which plaintiffs prevailed on a § 512(f) theory occurred relatively recently—one in 2014,¹⁵⁹ and one in 2015.¹⁶⁰

This category also revealed a surprising number of instances in which a § 512(f) claim was filed to prevent a copyright holder from issuing repeated takedown requests.¹⁶¹ This suggests at least a perceived inadequacy of the § 512(g) counter-notification procedure to protect users from the threat of repeated takedown requests. If the counter-notification procedure were enough to prevent copyright holders from submitting unsubstantiated takedown requests, there should be less § 512(f) claims seeking such remedies as temporary restraining orders and injunctions, at least in theory. Indeed, in one case involving two competitors, the plaintiff's request for injunctive relief was denied because the court found that the counter-notification procedure was already an adequate means of "mitigat[ing] lost business."¹⁶² Ironically, the DMCA is written to provide an extra layer of protection for copyright holders following counter-notification, guarding against the re-uploading of contested content if the copyright holder "has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity."¹⁶³ Perhaps the statute could be amended to provide similar protection to users, who seem driven to litigation to, at least in part, address the threat of repeated takedown requests.

Lastly, category two revealed a low incidence of § 512(f) claims arising from takedowns that were known or suspected to have resulted from automated processes. A few of the cases, however, had facts suggesting that automated processes may have been involved, even if the court in those cases did not suggest as much. One example is *Curtis v. Shinsachi Pharmaceutical Inc.*, in which the plaintiff secured a default judgment against a defendant that had issued takedown

158. See, e.g., Loren, *supra* note 16, at 745–46 ("If taken seriously, the misrepresentation claim has the potential to shape the behavior of copyright owners who wield the powerful sword of the takedown notice. To date, however, few misrepresentation claims have been brought, and the early interpretations of the provisions have limited their effectiveness in curbing abuse.")

159. *Curtis*, 45 F. Supp. 3d 1190.

160. *Automattic*, 82 F. Supp. 3d 1011.

161. See, e.g., *Flynn*, 2013 WL 5315959 at *2; *Design Furnishings*, 2010 WL 5418893 at *3; *Novotny*, 2006 WL 2335598 at *1.

162. *Curtis*, 45 F. Supp. 3d at 1204–05.

163. 17 U.S.C. § 512(g)(2)(C).

requests where no allegedly infringing content was even identified.¹⁶⁴ One interesting § 512(f) case that explicitly references automated takedown procedures is *Disney v. Hotfile*, which involves an ISP (as opposed to a user) and is described in more detail below.¹⁶⁵

c. When a Party Asserts Infringement and the Other Asserts Section 512(f) (“Category Three”)

The table below demonstrates the number of mixed infringement and § 512(f) cases that were discovered in the research.¹⁶⁶ There were four total cases found; the table below divides the data by examining the outcomes of the infringement claims and § 512(f) claims separately.

	<i>with counter- notification</i>	<i>counter- notification unclear</i>	<i>total # (of claims)</i>
<i>infringement claim fails</i>	0	2	2
<i>infringement claim succeeds</i>	0	1	1
<i>infringement claim unresolved</i>	1	0	1
<i>512(f) claim fails</i>	0	3	3
<i>512(f) claim succeeds</i>	0	0	0
<i>512(f) claim unresolved</i>	1	0	1
			8 (4 cases overall)

Figure 4. Category Three Findings

Generally, these cases represent instances in which both parties believe they have colorable claims; although in one case, the same party asserted both

164. *Curtis*, 45 F. Supp. 3d at 1199.

165. *Disney Enters., Inc. v. Hotfile Corp.*, No. 11-20427-CIV, 2013 WL 6336286 (S.D. Fla. Sept. 20, 2013).

166. The cases were: *TD Bank v. Hill*, Civ. No. 12-7188, 2015 WL 4523570 (D. N.J. July 27, 2015); *Shropshire v. Canning*, No. 10-CV-01941, 2011 WL 90136 (N.D. Cal. Jan. 11, 2011); *UMG Recordings, Inc. v. Augusto*, 558 F. Supp. 2d 1055 (C.D. Cal. 2008), *aff'd*, 628 F.3d 1175 (9th Cir. 2011); *Biosafe-One, Inc. v. Hawks*, 524 F. Supp. 2d 452 (S.D.N.Y. 2007).

infringement and § 512(f).¹⁶⁷ In that case, the plaintiff sued the defendant for copyright infringement after the defendant had posted an allegedly infringing video on YouTube, and the plaintiff also sued under § 512(f), asserting that the defendant misrepresented that his content was noninfringing when he sent a § 512(g) counter-notice to YouTube.¹⁶⁸ While this case ultimately settled, it presents an interesting scenario in which an alleged infringer could be held liable both for copyright infringement and for § 512(f) misrepresentation.

Perhaps unsurprisingly—and perhaps because the data set is so small—where both parties believe they have colorable claims, no conclusions can really be drawn as to the likelihood of success on the copyright infringement or § 512(f) claim. The party asserting § 512(f) was markedly less likely to succeed in these cases than in category two cases, but that is a logical result because in category two cases, the copyright holder chose not to litigate the issue of copyright infringement at all. This suggests that category two cases perhaps represent scenarios in which the underlying takedown request was more likely to be erroneous than in category three cases, because in category three cases, the copyright holder at least believes that she has a valid claim of copyright infringement. In theory, any copyright holder issuing a takedown notice should feel that she would have a colorable copyright infringement claim should the dispute reach litigation. The fact that the copyright holders in category two cases did not bring infringement claims could help explain why users were more likely to achieve success on their § 512(f) claims in category two cases than in category three cases. This perhaps suggests that where the copyright claim is weak, or where the connection between the copyrighted material and the allegedly-infringing material is tenuous, the takedown request is more likely to be illegitimate and the user's § 512(f) claim is stronger as a result.

d. A Case of Pushback on a Robo-Takedown Request

In *Disney Enterprises, Inc. v. Hotfile Corp.*,¹⁶⁹ five major film studios¹⁷⁰ sued online storage locker Hotfile and its operator for direct and secondary copyright infringement.¹⁷¹ Hotfile then filed a counterclaim relating to 890 takedown requests submitted by the plaintiffs, alleging § 512(f) abuse of the notice-and-takedown procedure.¹⁷² While this is a case of an ISP, not an individual user, pushing back on copyright holders, it presents very interesting legal questions because it specifically targets a robo-takedown regime.

167. See *Shropshire*, 2011 WL 90136.

168. *Id.*

169. 798 F. Supp. 2d 1303 (S.D. Fla. 2011) (“*Hotfile I*”).

170. The five major studios included Disney, Twentieth Century Fox, Universal, Columbia Pictures, and Warner Bros. *Id.* at 1306.

171. *Id.* at 1307.

172. *Disney Enters., Inc. v. Hotfile Corp.*, No. 11-20427-CIV, 2013 WL 6336286 at *14 (S.D. Fla. Sept. 20, 2013) (“*Hotfile II*”).

In a 2013 order on various motions for summary judgment, the court found the defendants vicariously liable, but also held that the defendants could proceed on their § 512(f) counterclaim at trial. In their counterclaim, the defendants asserted a willful blindness theory, “ask[ing] whether certain ‘egregious’ attributes of Warner’s system that might have prevented it from acquiring subjective knowledge . . . unjustly insulate Warner from liability for unreasonable mistakes.”¹⁷³ Even though the defendants were not entitled to safe harbor protections because they “lacked any meaningful policy to combat infringement,”¹⁷⁴ the court went one step beyond the defendants’ willful blindness theory and held that the defendants could still proceed to trial on their § 512(f) claim because “there is sufficient evidence in the record to suggest that Warner intentionally targeted files it knew it had no right to remove.”¹⁷⁵ The court seemed particularly concerned with the automated nature of Warner’s takedown practices, noting that although there was no known case “that actually address[es] the need for human review,” “Warner’s reliance on technology to accomplish the task might prevent it from forming any belief at all.”¹⁷⁶ The court went on to quote from an amicus brief filed in *Rossi*, in which it was argued that “computers conducting automated searches cannot form a belief consistent with the language of the DMCA, because they cannot distinguish between infringing content and content that merely contains words that suggest infringement.”¹⁷⁷

Even more surprisingly, in September 2014, a federal judge ordered that Warner release previously sealed details of its robo-takedown regime pursuant to Hotfile’s counterclaim.¹⁷⁸ The documents reveal the following about Warner’s robo-takedown regime:

Warner devotes the efforts of seven employees to online anti-piracy enforcement, hires third-party vendors, and, notably, uses the “common practice” of having “automated systems scan link sites and issue notifications of infringement to storage locker sites when infringing content is detected.” This last practice is apparently the method by which the counterclaim files were selected for deletion and requires some explanation.

In the automated review process, Warner’s employees first determine that a site is used for Internet piracy. Then they manually create programmable instructions and material criteria for “robots”—software programs that use keywords to search for content based on attributes such as the file’s title, genre, and year of release. The robots then, on their own, use search algorithms to spot URL links to infringing

173. *Id.* at *47.

174. *Id.* at *10.

175. *Id.* at *48.

176. *Id.* at *47. Notably, in dicta, the Ninth Circuit has opined that automated processes on their face do not trigger § 512(f) concerns. See *Lenz II*, 801 F.3d at 1135.

177. *Hotfile II*, 2013 WL 6336286, at *47 (internal quotations omitted).

178. Mitch Stoltz, *EFF Wins Release of Warner Bros. Documents on Robo-Takedown System*, ELEC. FRONTIER FOUND. (Sept. 26, 2014), <https://www.eff.org/deeplinks/2014/09/eff-wins-release-warner-bros-documents> [<https://perma.cc/5VLA-L3NT>].

content. The search instructions are refined based on how often they improperly detect non-Warner content that appears in the robots' search results.¹⁷⁹

Not surprisingly, the details of Warner's automated takedown process, including the use of the word "robots," did not appear in the original, sealed version of the order. While this case has since settled, the 2014 order opens the door for other judges to take a closer look at the robo-takedown regimes of copyright holders.

III. HARNESSING ROBOTS AS A FORCE FOR GOOD

It is still unclear how effective robo-takedown regimes are at targeting infringing material, and how much of the content that is removed pursuant to such requests is actually infringing. The litigation arising from user pushback on takedown requests generally suggests that perhaps the notice-and-takedown mechanism is working as planned; that is, fighting against piracy while minimizing the instances of erroneous takedowns. What is certain, however, is that there is evidence of at least some noninfringing content that is erroneously removed pursuant to robo-takedown requests.¹⁸⁰ Further, there is limited recourse for copyright holders that send overbroad requests, and thus little incentive for copyright holders to try to optimize their procedures in a way that limits the possibility of erroneous takedown requests. In a world where the use of automated takedown procedures is on the rise, it is necessary to equip users with the tools they need to fight back against erroneous takedown requests.

While robo-takedowns may be the best means available for dealing with rampant online piracy, copyright holders should at the very least be incentivized to make their procedures as optimal as possible. Such incentives should seek to result in the fewest possible number of erroneous requests, thereby striking a better balance between copyright holders and end-users.

The first step in addressing the problems inherent to the current notice-and-takedown environment is to shift the public perception away from viewing robo-takedown systems as categorically abusive. It is unhelpful to look at an instance of an overly broad takedown request as conclusive evidence of the abusive nature of such practices as a categorical matter because it ignores the legitimate aim of takedown procedures to curb online piracy. Instead, there must be a better way of describing the point at which a robo-takedown system actually veers so far away from its legitimate goal of combating digital piracy that it becomes an "abuse" of the § 512 notice-and-takedown provision. Reframing the issue as such would help to both create more productive discussion of the issue but also to better hold copyright holders accountable when they do, in fact, take advantage of the procedure.

179. Order Denying Summary Judgment on Hotfile Counterclaim at 29, *Disney Enters., Inc. v. Hotfile Corp.*, No. 11-20427-CIV, 2013 WL 6336286 (S.D. Fla. Sept. 20, 2013) ("*Hotfile II*"), <https://www.eff.org/document/order-denying-summary-judgment-hotfile-counterclaim-ecf-534>.

180. See *supra* Part II.C.

The next step is to empower users to push back when their content has been the target of an erroneous robo-takedown request. It is important both for individuals to understand their rights when their content is erroneously targeted by such requests and to have an efficient mechanism in place for users to push back against the removal of their content. This is particularly true because, as long as robo-takedown systems exist, there will remain the possibility that such processes will make mistakes and that overly broad requests will result.

Lastly, in response to the “whack-a-mole” problem in particular, technologies should be developed to ensure that material that is affirmatively identified as infringing stays off the Internet. This would help ensure that takedown requests actually target pirates and not innocent users, and could also mean that copyright holders are less tempted to employ automated processes in the first instance.

A. DRAWING A BETTER LINE BETWEEN “ABUSIVE” AND “NON-ABUSIVE” TAKEDOWN PRACTICES

The first step in creating a more optimal notice-and-takedown environment is to better define the point at which robo-takedown regimes actually become abusive. This would benefit multiple parties: users would have a better sense of when they might have a cognizable claim, or might feel more empowered in employing the counter-notification mechanism; ISPs would get less bad publicity for employing automated processes generally, allowing them to focus on improving their takedown and counter-notification policies; and copyright holders would be incentivized to optimize their procedures so that they are as narrowly-tailored as possible to capture instances of piracy while limiting the takedown of noninfringing content.

One extreme in drawing the line would be to say that robo-takedown practices are only abusive if the user can demonstrate that the copyright holder possessed subjective “bad faith” in issuing the request per *Rossi*. In fact, some commentators already adopt a § 512(f)-based standard.¹⁸¹ But, this would be an incredibly difficult standard for a user to meet and would likely fail to address the chilling effect that takedown requests currently have on free speech. On the other end of the extreme, robo-takedowns could be considered abusive once a robo-takedown request results in the removal of any noninfringing content. Thus, even if a user could not succeed on a § 512(f) claim against the copyright holder by demonstrating bad faith, the request would still be considered abusive by resulting in the removal of noninfringing content.¹⁸² While this would be a much easier standard for the user to meet, it would place an unduly onerous burden on copyright holders—who face the undeniable problem of rampant piracy online, including the

181. COPYRIGHT GREEN PAPER, *supra* note 11, at 57.

182. “[C]opyright holders may send insufficient or vague notices, and even send notices on suspicion of diligent investigation, without triggering § 512(f).” Urban & Quilter, *supra* note 104, at 629.

“whack-a-mole” problem—and ISPs—which are saddled with the responsibility of responding to an ever-increasing volume of takedown requests each day.

Perhaps the best option would be a middle ground between the two extremes. For example, a copyright holder could be said to abuse the notice-and-takedown provision if she employs automated processes that result in the issuance of takedown requests for content having nothing to do with the copyrighted material in question. Or, maybe abuse occurs where the requests frequently target content that traditionally fall under the category of “tolerated use”; for example, fan fiction websites or YouTube videos of people playing video games.¹⁸³ At any rate, there are many potential ways the discourse surrounding automated takedown regimes can be better framed so that copyright holders and ISPs are incentivized to minimize the risk of erroneous takedown requests and so that, when noninfringing content is in fact targeted, users know when to push back with counter-notification or litigation.

B. STRENGTHENING THE COUNTER-NOTIFICATION SYSTEM WITH USER EDUCATION AND EMPOWERMENT

Much literature has been devoted to ways in which automated takedown procedures necessarily result in the chilling of free speech and should, therefore, be disallowed or at least discouraged by the DMCA. Many of these proposals, however, ignore the reality that robo-takedowns are perhaps a necessary feature in today’s notice-and-takedown environment. Further, placing additional burdens on copyright holders and ISPs will make it easier for pirates to continue skirting the copyright laws and profiting off the creative content of others. Instead of focusing on ways to disincentivize the use of automated takedown procedures in the first instance, attention should instead be focused on improving the counter-notification procedure so that, when noninfringing content is erroneously targeted, the counter-notification procedure can become an effective tool for users to make sure their noninfringing content is protected.

A legislative approach could involve making the jurisdictional consent requirement of § 512(g) symmetrical or taking it out entirely. Currently, users wishing to serve counter-notifications under § 512(g) must submit to the court’s jurisdiction, but copyright holders submitting the initial takedown requests do not.¹⁸⁴ Making this requirement symmetrical would at least place the same jurisdictional requirement on copyright holders as on users, creating an even

183. For a discussion of “tolerated use,” see Tim Wu, *Tolerated Use*, 31 COLUM. J.L. & ARTS 617 (2008).

184. “[T]he DMCA provides explicitly that internet users . . . who wish to rebut a takedown notice must consent to the jurisdiction of a federal district court, but the statute does not require copyright owners who send takedown notices . . . to consent to personal jurisdiction. That difference must be viewed as intentional. If that result seems asymmetrical and unfair, then the problem should be resolved by Congress, not this court.” *Doe v. Geller*, 533 F. Supp. 2d 996, 1011 (N.D. Cal. 2008) (internal citations omitted).

playing field and making copyright holders think twice before submitting takedown requests that could result in the removal of noninfringing content. Currently, “the sending of a cease-and-desist letter into a forum is generally not considered sufficient to establish personal jurisdiction under the ‘effects test’ for purposeful availment in tort cases.”¹⁸⁵ The circuits vary considerably as to whether sending a takedown notice will confer personal jurisdiction on a copyright holder.¹⁸⁶ In fact, one case analyzed in the litigation research was dismissed because the defendant copyright holder had sent a takedown request from outside the United States and the court held that it therefore lacked personal and subject matter jurisdiction over the defendant.¹⁸⁷ Simply requiring copyright holders to fill out a form similar to that required of users could make them think twice before sending frivolous takedown requests. The jurisdiction requirement could also be taken out entirely, which would probably have the effect of making the counter-notification procedure seem less intimidating to the average user. This could be problematic, however, in situations where pirates who are not subject to the jurisdiction of U.S. courts follow the counter-notification procedure to prevent the removal of infringing material.

A policy-based approach to strengthening the counter-notification procedure would be to improve public education on the procedure and how to use it. ISPs, as well as Internet watchdogs like EFF and TorrentFreak, would be excellent and obvious fora for such information, but it would also benefit the copyright holders themselves to contribute to public education on the counter-notification procedure. As previously discussed, a lower incidence of erroneous takedowns would result in less bad press for copyright holders and would allow them to focus on optimizing automated takedown procedures.

Step one toward improving user education would be to help users better identify when they might have a good argument that their content is noninfringing, i.e., when they might have a good basis for challenging a request to take their content down. Part of this process could include providing information about the contours of copyright law generally so that users have a better sense of when their content may contain copyrighted material in the first instance. This would not only help users better understand when their content may have been erroneously targeted by a takedown request, but could also help users know when the content they post online might actually be infringing someone’s valid copyright. No vast discussion of copyright law would be required here to give users a better sense of when their content may contain copyrighted material; a simple checklist, for example, could suffice, as could a list of copyrighted material that is most often found in UGC content (e.g., a song created by someone other than the user). Next, users should

185. Loren, *supra* note 16, at 777.

186. See *Envtl. Graphics, LLC v. Med. Murals, LLC*, Civil No. 13-166 ADM/AJB, 2013 WL 3338779, at *4 (D. Minn. July 2, 2013) (noting that the Ninth and Tenth Circuits have found that an out-of-forum takedown request or “other third-party enforcement action” is enough to confer personal jurisdiction, and that the Federal Circuit test, by contrast, requires that the third party be located in the forum).

187. See *Geller*, 533 F. Supp. 2d 996.

be given a better sense of when they might have a good case for why their material is noninfringing. For instance, users should be explicitly informed that content that has nothing to do with the copyrighted material in question is obviously noninfringing and that such a scenario would present a great case for pushback on a takedown request. Also, content that obviously constitutes fair use could be identified—for example, parody videos. Of course, the notoriously murky “gray areas” of the fair use doctrine would be more difficult to explain, and would be harder to implement as part of a large-scale education objective.

The next step would be to educate the public on the how the counter-notification procedure works, what it entails, and what one’s likelihood of success is once it’s followed. Key to this effort is educating the public on the markedly low incidence of litigation that ensues once the counter-notification procedure is actually followed. The litigation analysis revealed only six cases of copyright infringement litigation arising after a user explicitly followed the counter-notification procedure (combining the results from categories one and three). This suggests that when the user has a reason to contest takedown of her material, there is at least a chance that the copyright holder will choose not to sue. Further, where a user successfully asserts a § 512(f) misrepresentation claim against a copyright holder, whether or not the user first followed the counter-notification procedure is something the court considers when determining the amount of damages to which the user is entitled.¹⁸⁸ Users should thus be encouraged to employ counter-notification when they think they might have a cognizable § 512(f) claim.

A final step might be for ISPs to better inform the public on their individual counter-notification policies (many of them are already beginning to do this)—or, better yet, for ISPs to adopt a uniform, across-the-board counter-notification policy and procedure. A uniform policy and procedure would result in less confusion for users and would make it more likely that users would actually follow the procedure where they have a good case of noninfringing use.

C. EMPLOYING TECHNOLOGY TO CREATE MORE COST-EFFICIENT “STAY DOWN” MECHANISMS

A final suggestion for improving the current robo-takedown environment—one that might actually lessen the incentive for copyright holders and ISPs to employ automated takedown procedures in the first place—is to create more efficient mechanisms to ensure that material found to be infringing stays down.¹⁸⁹ With the “whack-a-mole” problem addressed, copyright holders could rest assured that material determined to be infringing does not reappear moments after takedown in another location on the same site.

Perhaps the best possible solution would be for ISPs to universally adopt a filtering approach by developing a screening process at the moment of upload that

188. See, e.g., *Automatic Inc. v. Steiner*, 82 F. Supp. 3d 1011, 1029 (N.D. Cal. 2015).

189. *Hearing, supra* note 99, at 10 (statement of Sean M. O’Connor, Professor of Law).

blocks the re-upload of material previously determined to be infringing.¹⁹⁰ This technique, referred to as “notice and stay-down,”¹⁹¹ would be technologically similar to some filtering systems that are already in place for all uploads on certain sites. YouTube’s Content ID system is one example of technology that exists today that is able, in theory at least, to identify potentially infringing content at the moment of upload.¹⁹² To make the technology more precise, however, filtration for certain content could only occur once the ISP has identified infringing material and removed it pursuant to a takedown request. While it is still possible that some material could be misidentified at the initial takedown stage, thus resulting in the blocking of noninfringing content, the user in that scenario would still be able to undergo the counter-notification procedure to get her content reinstated.

The technology for this kind of filtering already exists and involves processes like watermarking or fingerprinting to properly identify content that has already been determined to be infringing.¹⁹³ Further, filtration methods have already received support from a variety of companies and are currently employed to various degrees on numerous UGC sites.¹⁹⁴

CONCLUSION

So, in the battle of robots versus pirates, who will prevail?

The use of robo-takedown regimes is controversial, but perhaps that is because the effects of such regimes are not entirely understood, or because copyright holders and ISPs have not yet figured out a way to employ them effectively. While there is clearly evidence of instances in which copyright holders employ overly broad or “abusive” takedown practices, there is also evidence to suggest that such practices can be turned into a force for good.

Thus, the problem with the state of robo-takedowns today is twofold. First, there is at least some evidence of overbroad takedown requests where robo-takedowns result in the removal of noninfringing content. This is particularly problematic in the digital world, where the preemptive removal of allegedly infringing content results in the chilling of free speech where the content turns out, in fact, to be noninfringing. Second, the mechanisms available for users to push back on takedown requests targeting their content are not entirely viable. Even though it is unclear what proportion of all takedown requests result in the removal of noninfringing material, when it does happen, users need a way to fight back.

190. “ISPs can at least in theory filter at the network level by screening all incoming network traffic to look for unique identifying marks, which could be assigned to each piece of digital content, to determine whether transmissions are authorized.” COPYRIGHT GREEN PAPER, *supra* note 11, at 65.

191. *Hearing*, *supra* note 99, at 14 (statement of Sean M. O’Connor, Professor of Law).

192. “YouTube’s Content ID digital fingerprinting system . . . allows right holders to submit metadata and reference files for content they own, which are compared to videos posted on YouTube.” COPYRIGHT GREEN PAPER, *supra* note 11, at 66.

193. COPYRIGHT GREEN PAPER, *supra* note 11, at 65.

194. COPYRIGHT GREEN PAPER, *supra* note 11, at 65–66.

It is therefore imperative that critics begin to at least consider the possibility that robo-takedown regimes might be the most efficient tool against piracy in the digital age, and that public discourse shift from a categorical dismissal of automated procedures toward more constructive efforts to improve them. Defining the point at which a takedown regime actually becomes “abusive” is the first step in addressing this problem. This will both help users know when they are likely to succeed in pushing back and will incentivize copyright holders and ISPs to optimize their procedures. Once this is accomplished, a variety of other strategies can be employed to create a better notice-and-takedown environment for all parties. These suggestions include amending the DMCA, implementing policies of user education and empowerment, and harnessing the power of technology to make sure content that is found to be infringing stays down. By turning robots into a force for good, it is possible to achieve the correct balance between the interests of copyright holders, ISPs, and users.