I. Background

Congress enacted section 512 in 1998 as part of the Digital Millennium Copyright Act ("DMCA"). At that time, less than 5% of the world’s population used the internet, and bulletin board services were the popular online platforms. Even then, however, Congress recognized that “the [i]nternet . . . made it possible for information—including valuable American copyrighted works—to flow around the globe in a matter of hours,” and, as a consequence, copyright law needed to be “set . . . up to meet the promise and the challenge of the digital world.”

In enacting section 512, Congress created a system for copyright owners and online entities to address online infringement, including limitations on liability for compliant service providers to help foster the growth of Internet-based services. The system reflected Congress’ recognition that the same innovative advances in technology that would expand opportunities to reproduce and disseminate content could also facilitate exponential growth in copyright infringement. Accordingly, section 512 was intended by Congress to provide strong incentives for service providers and copyright owners to “cooperate to detect and deal with copyright infringements that take place in the digital networked environment,” as well as to offer greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities.

Congress was especially concerned about the liability of online service providers for infringing activities of third parties occurring on or through their services. To address this issue, Congress created a set of “safe harbors”—i.e., limitations on copyright infringement liability—for certain common activities of service providers. But the safe harbors are not automatic. To qualify for protection from infringement liability, a service provider must fulfill certain requirements, generally consisting of implementing measures to expeditiously address online copyright infringement.

Recent research suggests that the volume of infringing material accessed via the Internet more than doubled from 2010 to 2012, and that nearly one-quarter of all Internet bandwidth in North America, Europe, and Asia is devoted to hosting, sharing, and acquiring infringing material. While Congress clearly understood that it would be essential to address online infringement as the Internet continued to grow, it was likely difficult to anticipate the online world as we now know it—where, each day, users post hundreds of millions of photos, videos, and other items, and service providers receive over a million notices of alleged infringement.

As observed by the House Judiciary Committee’s Ranking Member in the course of the Committee’s ongoing multi-year review of the Copyright Act, and consistent with the testimony of the Register of Copyrights in that hearing, the operation of section 512 poses policy issues that warrant study and analysis. Section 512 has also been a focus of the U.S. Department of Commerce in recent years, which has noted ambiguities in the application of

---

2 See Internet Users, Internet Live Stats (Dec. 1, 2015), http://www.internetlivestats.com/internet-users/#trend (In 1998, there were only 188 million internet users; today, there are over 3.23 billion.).
5 See H.R. Rep. No. 105–551, pt. 2, at 21 (1998) (noting that the DMCA, including section 512 of title 17, "balances[s] the interests of content owners, on-line and other service providers, and information users in a way that will foster the continued development of electronic commerce and the growth of the [i]nternet").
the safe harbor and encouraged service providers and rightsholders to discuss and pursue voluntary improvements.10

The present study will review the statutory requirements of section 512 and evaluate its current effectiveness and impact on those who rely upon it. The key aspects of section 512 that are the subject of this review, including notable legal and practical developments, are summarized below.

A. Overview of Section 512 Safe Harbors

Section 512 provides safe harbors from infringement liability for online service providers that are engaged in qualifying activities and that also meet certain eligibility requirements. There are four distinct safe harbors, detailed in sections 512(a), (b), (c), and (d), respectively. These safe harbors are available when a service provider engages in one or more of the following corresponding activities: (a) Serving as a conduit for the automatic online transmission of material as directed by third parties; (b) caching (i.e., temporarily storing) material that is being transmitted automatically over the internet from one third party to another; (c) storing (i.e., hosting) material at the direction of a user on a service provider’s system or network; or (d) referring or linking users to online sites using information location tools (e.g., a search engine).

A service provider that meets the relevant eligibility requirements for one or more of the safe harbors is not liable for monetary relief and is subject only to limited injunctive relief for infringing activities conducted on or through its system or network.11 In the case of a service provider that qualifies for a safe harbor under 512(b), (c), or (d), this injunctive relief is limited to: (1) Disabling access to infringing material; (2) terminating the infringer’s account(s); and (3) providing such other relief as may be necessary to address infringement at a particular online location; provided, however, that the relief is “‘the least burdensome [form of relief] to the service provider.’”12 For a service provider that qualifies for the 512(a) safe harbor, the court may order only termination of an infringer’s account(s) or blocking of access to a “specific, identified, online location outside the United States.”13

In order to qualify for the limitation on liability provided under section 512(a), (b), (c), or (d), the service provider must comply with certain threshold requirements. Two of these requirements apply to all four safe harbors: (1) The adoption and reasonable implementation of a policy to terminate “repeat infringers”;14 and (2) the accommodation of “standard technical measures” that identify or protect copyrighted works and have been developed according to broad consensus between copyright owners and service providers, to the extent any such measures exist.15 A service provider that acts as a mere conduit for online transmissions qualifies for the limitation on liability provided by section 512(a) if the provider satisfies these two threshold requirements.

Service providers seeking protection under the safe harbors in section 512(b), (c), or (d), however, must, in addition, maintain a compliant notice-and-takedown process by responding expeditiously to remove or disable access to material claimed to be infringing upon receipt of proper notice from a copyright owner or the owner’s authorized agent.16 A service provider seeking to avail itself of the section 512(c) safe harbor for user-posted content is further required to designate an agent to receive notifications of claimed infringement and provide contact information for the agent on its Web site and to the Copyright Office, which, in turn, is to maintain a public directory of such agents.17 The statute prescribes that a copyright owner’s takedown notice must include

```
11 17 U.S.C. 512(a)-(d).
12 Id. at 512(j)(1)(A).
13 Id. at 512(j)(1)(B).
14 A service provider must adopt, “reasonably implement[,] and inform subscribers and account holders of a policy that provides for the termination in appropriate circumstances of . . . repeat infringers.” Id. at 512(j)(1)(A).
15 Id. at 512(j)(1)(B), (i)(2).
16 Id. at 512(b)(2)(E), (c)(1)(C), (d)(3). The process for notification under the 512(c) and (d) safe harbors is set out in 512(c)(3); the process differs somewhat under the 512(d) safe harbor in that, in addition to following the requirements of 512(c)(3), the complaining party must also confirm that the content or link has been removed or disabled by the originating site or that a court has ordered that it be removed or disabled.
17 Id. at 512(c)(2). Although section 512(d) does not itself express providers to designate an agent to receive notifications of infringement, it incorporates the notice provisions of section 512(c)(3), which require that notices be sent to “the designated agent of the service provider.” The statutory scheme thus indicates that service providers operating under section 512(d) would also designate agents to receive takedown notices. See id. at 512(c)(3).
```

“substantially the following”: (i) The signature of the copyright owner or an authorized agent (i.e., the complaining party); (ii) identification of the copyrighted work claimed to have been infringed, or, if multiple works are on a single site, “a representative list of such works”; (iii) identification of the infringing material or activity (or the reference or link to such material) and “information reasonably sufficient” to permit the service provider to locate the material (or the reference or link); (iv) contact information for the complaining party; (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”; and (vi) a statement that the information is accurate and, under penalty of perjury, that the complaining party is authorized to act on behalf of the copyright owner.18 A copyright owner’s communication that does not substantially comply with these criteria will not serve as effective notice for purposes of the statutory process.19 Further, under section 512(f), as discussed more fully below, “[a]ny person who knowingly materially misrepresents . . . that material or activity is infringing” can be held liable for any damages, including costs and attorneys’ fees, incurred by an alleged infringer who is injured by the misrepresentation.

In addition to responding to takedown notices, service providers that seek protection under the section 512(c) and (d) safe harbors must also act expeditiously to remove or disable access to material when they have “actual knowledge” of infringement or, in the absence of such actual knowledge, when they have “aware[ness] of facts or circumstances from which infringing activity is apparent”—the “aware[ness]” standard often referred to as “red flag” knowledge.20 But, while service providers are not free to ignore infringement of which they have actual or red flag knowledge, section 512 at the same time provides that an online entity has no duty to “monitor[] its service or affirmatively seek[] facts indicating

```
18 Id. at 512(c)(3)(A)(i)-(vi).
19 See id. at 512(c)(3)(B)(i) (“A notification . . . that fails to comply substantially . . . shall not be considered . . . in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.”); see also Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1112–14 (9th Cir. 2007) (“CCBill LLC”) (“[A] service provider will not be deemed to have notice of infringement when the notification . . . fails to comply substantially with all the provisions of 17 U.S.C. 512(c)(3)(A).”).
20 See 17 U.S.C. 512(c), (d).
```
infringing activity, except to the extent consistent with a standard technical measure.” 21

Finally, to qualify for the section 512(c) and (d) safe harbors, a service provider must not “receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity.” 22 The statutory financial benefit/right to control test does not incorporate a knowledge element. 23

In addition to the general limitations on infringement liability, the statute provides specific protections for service providers that remove material in response to takedown notices, as well as for users who post material that is claimed to be infringing. Under section 512, a service provider is not liable for the good-faith removal or disabling of access to material “claimed to be infringing or based on facts or circumstances from which infringing activity is apparent”—even material not ultimately found to be infringing—so long as the provider takes reasonable steps to promptly notify the user who posted the material that it has been removed and also complies, as applicable, with a statutory counter-notification process. 24

Section 512(g) allows a user whose content has been removed in response to a takedown notice to submit a counter notification to a service provider’s designated agent requesting that the content be reposted. The counter notification must include: (i) the signature of the subscriber (i.e., the counter-notifying party); (ii) identification of the material that was removed or to which access was disabled, as well as the location where it previously appeared; (iii) 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”; and (iv) the subscriber’s contact information, as well as a statement that the subscriber consents to the jurisdiction of the federal district court for the relevant judicial district and agrees to accept service of process from the party who provided the takedown notice (or that party’s agent). 25 To preserve its safe harbor immunity, the service provider must republish the content within 10 to 14 business days of receiving the counter notice unless the service provider first receives notice from the party who provided the takedown notice that a judicial action has been filed “seeking . . . to restrain the subscriber from engaging in infringing activity relating to the material on the service provider’s system or network.” 26 As in the case of misrepresentations in takedown notices, under section 512(f), any person who knowingly materially misrepresents that “material or activity was removed or disabled by mistake or misidentification” may be held liable for monetary damages, including costs and attorneys’ fees. 27

B. Key Developments

Since the enactment of section 512, stakeholders have adopted practices and systems to implement it, and courts have been called upon to interpret its provisions—from eligibility for safe harbors to the requirements for valid takedown notices to the standards that govern misrepresentations in the notification process. Some stakeholders have created best practices, entered into voluntary agreements to streamline enforcement procedures, and/or pursued other non-judicial approaches. Notwithstanding these developments, many on both sides of the equation express significant frustration with the process. A brief overview of the most salient issues follows.

Notice-and-Takedown Process

Today, copyright owners send takedown notices requesting service providers to remove and disable access to hundreds of millions of instances of alleged infringement each year. 28 The number of removal requests sent to service providers has increased dramatically since the enactment of section 512. For example, one search engine now “receive[s] removal requests for more URLs every week than [it] did . . . from 1998 to 2010 combined.” 29 Technology has come to play a significant role in the notice-and-takedown process, as automated processes that use fingerprinting, hash values, and keyword/metadata searches can identify movies, sound recordings, and other types of content that are being posted and disseminated. 30 But regardless of increasing technological capabilities, stakeholders frequently voice concerns about the efficiency and efficacy—not to mention the overall sustainability—of the system. 31

Many smaller copyright owners, for example, lack access to third-party services and sophisticated tools with which to identify infringing uses, which can be costly, and must instead rely on manual search and notification processes 32—an effort that has been likened to “trying to empty the ocean with a teaspoon.” 33 In addition to the burden of policing infringement across the internet, copyright owners complain that material they succeed in having taken down is often promptly reposted on the same site—the so-called “whack-a-mole” problem. 34 Under section 512 as it has been interpreted, providers are not required to filter out or prevent the reposting of copyrighted content

21 Id. at 512(g)(2)(C).
22 Id. at 512(f).
24 See Section 512 Hearing at 9 (written statement of Sean M. O’Connor, Entrepreneurial Law Clinic, University of Washington (Seattle)) (“[T]here are takedown notices now filed on millions of posts every month. That is clearly unsustainable.”); Copyright Policy, Creativity, and Innovation in the Digital Economy 56 (“[R]ight holders and ISPs alike have identified respects in which the notice-and-takedown system’s operation can become unwieldy or burdensome.”).
25 See Section 512 Hearing at 100 (statement of Rep. Doug Collins) (“[I]ndividual songwriters and the independent filmmakers . . . often have limited or no technical expertise or software at their disposal . . .”); id. at 88–89 (2014) (written statement of Sandra Aistars, Copyright Alliance) (Independent authors and creators “lack the resources of corporate copyright owners” or instead issue “takedown notices themselves, taking time away from their creative pursuits.”).
27 Section 512 Hearing at 35 (written statement of Paul Doda, Elsevier) (“The “same books are repeatedly re-uploaded on the same site hundreds of times after being taken down . . .”); id. at 57 (written statement of Maria Schneider, musician) (“As fast as I take my music down, it reappears again on the same site—an endless whac-a-mole game.”).
28 Id. at 512(m)(1).
29 Id. at 512(c)(1)(B), (d)(2).
30 See Section 512 Hearing at 100 (written statement of Rep. Doug Collins) (“[I]ndividual songwriters and the independent filmmakers . . . often have limited or no technical expertise or software at their disposal . . .”); id. at 88–89 (2014) (written statement of Sandra Aistars, Copyright Alliance) (Independent authors and creators “lack the resources of corporate copyright owners” or instead issue “takedown notices themselves, taking time away from their creative pursuits.”).
32 Section 512 Hearing at 35 (written statement of Paul Doda, Elsevier) (“The “same books are repeatedly re-uploaded on the same site hundreds of times after being taken down . . .”); id. at 57 (written statement of Maria Schneider, musician) (“As fast as I take my music down, it reappears again on the same site—an endless whac-a-mole game.”).
through the use of content identification technologies or other means.\textsuperscript{35} Accordingly, some have proposed that the notice-and-takedown procedure be revised to become a “notice-and-stay-down” procedure—that is, once a service provider receives an effective and uncontested takedown notice for a particular work, the provider should be required to make commercially reasonable efforts to keep that work from reappearing on its site.\textsuperscript{36} Others, however, pointing to the very substantial efforts—especially of larger service providers—to respond promptly to takedown notices, are of the view that the existing system has “scaled well” over time to address the large volume of takedown notices, and does not need to be changed.\textsuperscript{37}

Of course, the burdens of the notice-and-takedown process do not fall on copyright owners alone. Service providers must devote the time and resources necessary to respond to the increasing number of takedown notices sent each day. Smaller providers, in particular, may find the task to be a daunting one.\textsuperscript{38} In addition, service providers complain that some notices do not meet the statutory requirements or, as discussed below, concern materials and activities that are not in fact infringing.

Since the passage of the DMCA, courts have been called upon to address the elements required for an “effective”—i.e., valid—takedown notice. Looking to section 512’s requirement to provide “information reasonably sufficient to permit the service provider to locate the material,” courts have generally required a high degree of specificity, such as the particular link, or uniform resource locator (“URL”), where the infringing material is found.\textsuperscript{39} Likewise, service providers often request that the specific URL for each allegedly infringing use be included in a takedown notice.\textsuperscript{40} Such a requirement can be burdensome in the case of a notice that references a large number of infringements at multiple locations throughout the same site. Additionally, copyright owners question whether this level of specificity is in conflict with the statute’s express language allowing complaining parties to submit a “representative list” of works alleged to be infringed “at a single online site.” In addition, there is debate about whether search engine services must disable access to (e.g., “de-list”) entire sites that copyright owners report as consisting largely of infringing material.\textsuperscript{41} While the legislative history of section 512(d) observes that “safe harbor status for a provider that views [a pirate] site and then establishes a link to it would not be appropriate,”\textsuperscript{42} service providers assert that de-listing could lead to censorship, and yet still not effectively address infringement, because the site would remain online.\textsuperscript{43}

Knowledge Standards

A good deal of litigation relating to section 512 to date has focused on the legal standards for determining when a service provider has sufficient knowledge or awareness to require it to remove or disable infringing material in order to remain eligible for the safe harbor protections of section 512(c) or (d). Courts have held “actual knowledge” to require evidence that the service provider subjectively knew that specific material on its site infringed copyright.\textsuperscript{44} Alternatively, actual knowledge can be demonstrated with evidence that a service provider received information about specific infringing material through a statutorily effective takedown notice, i.e., a notice that includes “substantially” all of the information required under section 512(c).\textsuperscript{45}

Courts have also recognized the common law doctrine of willful blindness in addressing whether a service provider has actual knowledge of infringement.\textsuperscript{46} A service provider is considered to have engaged in willful blindness when it is “aware of a high probability of infringement and has ‘consciously avoided confirming that fact.’”\textsuperscript{47} Accordingly, courts have held that a service provider’s willful blindness to infringement on its site and failure to remove or disable access to infringing material can disqualify it from the “safe harbor.”\textsuperscript{48}
from the protections of a section 512 safe harbor. As also noted above, sections 512(c) and (d) require a service provider to disable access to material or activity if it has “red flag” knowledge, i.e., is aware of “facts or circumstances from which infringing activity is apparent.” In enacting the statute, Congress expressed that “a service provider [has] no obligation to seek out copyright infringement, but it [does] not qualify for the safe harbor if it . . . turn[s] a blind eye to ‘red flags’ of obvious infringement.” The legislative history of section 512 also suggests Congress’ view that the red flag test “has both a subjective and an objective element . . . the subjective awareness of the service provider of the facts or circumstances in question . . . [and the objective assessment of] whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances.” With regard to information location tools, for example, Congress observed that if “an [Internet] site is obviously pirate, then seeing it is a ‘red flag.’” Copyright owners have argued that Congress’ intent in creating the red flag test was to “require[ ] less specificity than the actual knowledge” standard and to prevent service providers from qualifying for safe harbor protection when they are aware of widespread infringement. Courts, however, have largely rejected the notion that a general awareness of infringement is sufficient to establish red flag knowledge. Instead, courts have held that red flag knowledge requires “knowledge of specific and identifiable infringements” because, in order to retain the protection of the safe harbor, the service provider is required to expeditiously “remove or disable ‘the [infringing] material.’”

In assessing these knowledge requirements, courts have also looked to the language of section 512(m), which states that “[n]othing in section 512 conditions the availability of safe harbor protection on ‘a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure.’” Based on this language, courts have concluded that “the DMCA . . . place[s] the burden of policing copyright infringement . . . squarely on the owners of the copyright.”

Financial Benefit/Right To Control

Litigation regarding the Section 512(c) and (d) safe harbors has also addressed what it means for a service provider to receive a “financial benefit directly attributable” to infringing activity where it has the “right and ability to control” such activity. Like the traditional standard for vicarious liability under common law, the financial benefit/right to control test has been held not to turn on a service provider’s knowledge of infringement. But courts have also indicated that “right and ability to control” in the context of section 512 means that the service provider “‘exert[s] substantial . . . control’ over the infringing activity.”

Copyright owners have argued that Congress’ intent in creating the red flag test was to “require[ ] less specificity than the actual knowledge” standard and to prevent service providers from qualifying for safe harbor protection when they are aware of widespread infringement. Courts, however, have largely rejected the notion that a general awareness of infringement is sufficient to establish red flag knowledge. Instead, courts have held that red flag knowledge requires “knowledge of specific and identifiable infringements” because, in order to retain the protection of the safe harbor, the service provider is required to expeditiously “remove or disable ‘the [infringing] material.’”

52 Id. at 53; S. Rep. No. 105–190, at 44 (1998); accord Viacom, 676 F.3d at 31.
53 H.R. Rep. No. 105–551, pt. 2, at 58 (1998); see also Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020, 1043 (9th Cir. 2013) (“Fung”) (finding that a service provider had red flag knowledge where “material in question was sufficiently current and well-known that it would have been objectively obvious to a reasonable person that the material was copyrighted and not licensed to random members of the public.”).
54 Viacom, 676 F.3d at 31–32 (internal quotations omitted).
55 See, e.g., UMG Recordings, 718 F.3d at 1022 (quoting CCBill LLC, 488 F.3d at 1113) (“CCBill LLC”) (noting that financial benefit is not established through a “one-time set-up fee [or] flat, periodic payments for service from a person engaging in infringing activities.”).
56 See, e.g., Viacom, 676 F.3d at 37.
58 See Viacom, 676 F.3d at 36–38 (2d Cir. 2012) (“17 U.S.C. 512(c)(1)(B) does not include a specific knowledge requirement because to ‘import[] a specific knowledge requirement into [17 U.S.C. 512(c)(1)(A)]’ . . . [is] ‘inconsistent with the legislative history’.”) (quoting Viacom, 676 F.3d at 31–32).
60 Fung, 710 F.3d at 1043; accord Viacom, 676 F.3d at 38 & n.13 ( “[C]ontrol may exist where the service provider is ‘actively involved in the listing, bidding, sale and delivery’ of items.”) (quoting Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082, 1094 (C.D. Cal. 2001)); Cybernet Ventures, 213 F.3d Supp. 2d at 1173 (finding that service provider had control where it required User Web sites to comply with “detailed instructions regarding issues of layout, appearance, and content”).
61 See, e.g., Viacom, 676 F.3d at 37.
63 CCBill LLC, 488 F.3d at 1117; Ellison v. Robertson, 357 F.3d 1072, 1079 (9th Cir. 2004).
64 Fung, 710 F.3d at 1045–46.
held that a reasonable policy, at a minimum, must provide a mechanism to identify and keep a record of users responsible for files referenced in takedown notices and, ‘‘under ‘‘appropriate circumstances,’ ’’ result in termination of ‘‘users who repeatedly or blatantly infringe copyright.’’

Misuse of Takedown Process

Service providers and advocacy groups have raised concerns about fraudulent and abusive section 512 notices that may restrain fair use, free speech, or otherwise misuse the notice-and-takedown process. Some of the concerns arise from takedown notices for content that appears to constitute an obvious fair use of a copyright work. Others relate to efforts to remove criticism or commentary—such as negative reviews—under the guise of criticism or commentary, such as “knowingly materially misrepresents” in a takedown notice that material is infringing, or, in a counter notification, was wrongly removed.77

In a number of cases challenging the validity of takedown notices, courts have fashioned the meaning and application of section 512(f). For example, courts have held that the “good faith belief” requirement of section 512(c)(3)(A)(v) “encompasses a subjective, rather than objective standard”; that is, the sender is not responsible for an “unknowing mistake,” even if the sender’s assessment of infringement was objectively unreasonable.78 But it has also been held that before sending a takedown notice, the complaining party must “consider the existence of fair use” in forming the subjective good faith belief that the use is not authorized by the law.79 The need to consider fair use may present challenges in the context of automated takedown processes relied upon by copyright owners to address large-volume infringements, including how such processes might be calibrated to accommodate this requirement and the necessity, if any, for human review.80

Voluntary Measures

While interested parties continue to test and clarify aspects of section 512 in the courts, some stakeholders have chosen to work together to develop voluntary protocols and best practices to avoid litigation, improve online enforcement, and protect free speech and innovation. Several of these initiatives have been undertaken with the support of the U.S. government, including the Copyright Alert System, an effort supported by the U.S. Intellectual Property Enforcement Coordinator (“IPEC”),81 and the DMCA Notice-and-Takedown Procedures: List of Good, Bad, and Situational Practices, stemming from the efforts of the Internet Policy Task Force,82 both of which seek to improve the efficiency and effectiveness of notice-and-takedown procedures, as well as the IPEC-led Payment Processor Best Practices, which seeks to cut off revenue to sites that promote infringement.83 Other multistakeholder initiatives include the Trustworthy Accountability Group certification process, aimed at curbing ad revenue supporting piracy Web sites,84 and the Principles for User Generated Content Services, which sets forth agreed principles for screening and addressing infringing content.85

II. Subjects of Inquiry

The Copyright Office seeks public input, including, where available, empirical data on the efficiency and effectiveness of section 512 for owners and users of copyrighted works and the overall sustainability of the system if, as appears likely, the volume of takedown notices continues to increase. The Office invites written comments in particular on the subjects below. A party choosing to respond to this Notice of Inquiry need not address every subject, but the Office requests that responding parties clearly identify and separately address each

70 See, e.g., Phi Psi v. Google, 488 F.3d at 1109 (internal citation omitted); see also Hoofdir. No. 11–2047–CIV, 2013 WL 6336286, at *21.
71 See, e.g., Section 512 Hearing at 48, 63–67, 246–47 (written statements of Katherine Oyama, Google Inc.; Paul Sieminski, Automattic Inc.; and Library Copyright Alliance) (discussing misuse of takedown process).
72 See, e.g., id. at 65 (written statement of Paul Sieminski, Automattic Inc.) (noting concern for “companies who use DMCA notices specifically against content that makes use of their copyrighted material as part of a criticism or negative review—which is classic fair use”).
73 See, e.g., Automattic Inc. v. Steiner, 82 F. Supp. 3d 1011, 1016 (N.D. Cal. 2015) (entering default judgment against the submitter of takedown notices for knowingly materially misrepresenting that a blog infringed its press release); Online Policy Grp. v. Diebold, Inc., 337 F. Supp. 2d 1195, 1204 (N.D. Cal. 2005) (machine manufacturer liable under section 512(f) for “knowingly materially misrepresent[ing]” that publication of material was infringing).
74 See, e.g., Brief for Org. for Transformative Works et al. as Amici Curiae Supporting Appellee and Cross-Appellant at 16, Lenz v. Universal Music Corp., 801 F.3d 1129, 1134 (9th Cir. 2015) (naming 13–16106, 13–16107) (noting that creators worry about sending a counter notice because they may have to provide their real names and addresses or become subject to a lawsuit they cannot afford).
77 Id. at 512(g)(3)(C).
78 Id. at 512(i).
79 Rossi v. Motion Picture Ass’n of Am., Inc., 391 F.3d 1000, 1004–05 (9th Cir. 2004); accord Lenz v. Universal Music Corp., 801 F.3d 1126, 1134 (9th Cir. 2015). The Rossi and Lenz courts reasoned that to hold otherwise would conflict with Congress’ intent that a copyright owner only be penalized for “knowing” misrepresentations. Rossi, 391 F.3d at 1004–05; accord Lenz, 801 F.3d at 1134.
80 Lenz, 801 F.3d at 1134.
81 See id. at 1135–36. In Lenz, the Ninth Circuit was “mindful of the pressing crush of voluminous infringing content that copyright holders face,” and noted, “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.” Id. at 1135. The court further addressed how an algorithm might accommodate fair use, observing that it was “unaware of any [court] decision to date that actually addressed the need for human review.” Id.
numbered subject for which a response is submitted.

General Effectiveness of Safe Harbors
1. Are the section 512 safe harbors working as Congress intended?
2. Have courts properly construed the entities and activities covered by the section 512 safe harbors?
3. How have section 512’s limitations on liability for online service providers impacted the growth and development of online services?
4. How have section 512’s limitations on liability for online service providers impacted the protection and value of copyrighted works, including licensing markets for such works?
5. Do the section 512 safe harbors strike the correct balance between copyright owners and online service providers?

Notice-and-Takedown Process
6. How effective is section 512’s notice-and-takedown process for addressing online infringement?
7. How efficient or burdensome is section 512’s notice-and-takedown process for addressing online infringement? Is it a workable solution over the long run?
8. In what ways does the process work differently for individuals, small-scale entities, and/or large-scale entities that are sending and/or receiving takedown notices?
9. Please address the role of both “human” and automated notice-and-takedown processes under section 512, including their respective feasibility, benefits, and limitations.
10. Does the notice-and-takedown process sufficiently address the reappearance of infringing material previously removed by a service provider in response to a notice? If not, what should be done to address this concern?
11. Are there technologies or processes that would improve the efficiency and/or effectiveness of the notice-and-takedown process?
12. Does the notice-and-takedown process sufficiently protect against fraudulent, abusive or unfounded notices? If not, what should be done to address this concern?
13. Has section 512(d), which addresses “information location tools,” been a useful mechanism to address infringement that occurs as a result of a service provider’s referring or linking to infringing content? If not, what should be done to address this concern?
14. Have courts properly interpreted the meaning of “representative list” under section 512(c)(3)(A)(ii)? If not, what should be done to address this concern?
15. Please describe, and assess the effectiveness or ineffectiveness of, voluntary measures and best practices—including financial measures, content “filtering” and takedown procedures—that have been undertaken by interested parties to supplement or improve the efficacy of section 512’s notice-and-takedown process.

Counter Notifications
16. How effective is the counter-notification process for addressing false and mistaken assertions of infringement?
17. How efficient or burdensome is the counter-notification process for users and service providers? Is it a workable solution over the long run?
18. In what ways does the process work differently for individuals, small-scale entities, and/or large-scale entities that are sending and/or receiving counter notifications?

Legal Standards
19. Assess courts’ interpretations of the “actual” and “red flag” knowledge standards under the section 512 safe harbors, including the role of “willful blindness” and section 512(m)(1) (limiting the duty of a service provider to monitor for infringement activity) in such analyses. How are judicial interpretations impacting the effectiveness of section 512?
20. Assess courts’ interpretations of the “financial benefit” and “right and ability to control” standards under the section 512 safe harbors. How are judicial interpretations impacting the effectiveness of section 512?
21. Describe any other judicial interpretations of section 512 that impact its effectiveness, and why.

Repeat Infringers
22. Describe and address the effectiveness of repeat infringer policies as referenced in section 512(i)(A).
23. Is there sufficient clarity in the law as to what constitutes a repeat infringer policy for purposes of section 512’s safe harbors? If not, what should be done to address this concern?
24. Does section 512(i) concerning service providers’ accommodation of “standard technical measures” (including the definition of such measures set forth in section 512(i)(2)) encourage or discourage the use of technologies to address online infringement?
25. Are there any existing or emerging “standard technical measures” that could or should apply to obtain the benefits of section 512’s safe harbors?

Remedies
26. Is section 512(g)(2)(C), which requires a copyright owner to bring a federal lawsuit within ten business days to keep allegedly infringing content offline—and a counter-notifying party to defend any such lawsuit—a reasonable and effective provision? If not, how might it be improved?
27. Is the limited injunctive relief available under section 512(j) a sufficient and effective remedy to address the posting of infringing material?
28. Are the remedies for misrepresentation set forth in section 512(f) sufficient to deter and address fraudulent or abusive notices and counter notifications?

Other Issues
29. Please provide any statistical or economic reports or studies that demonstrate the effectiveness, ineffectiveness, and/or impact of section 512’s safe harbors.
30. Please identify and describe any pertinent issues not referenced above that the Copyright Office should consider in conducting its study.


Maria A. Pallante,
Register of Copyrights, U.S. Copyright Office.

BILLY CODE 1410-30-P

MILLENNIUM CHALLENGE CORPORATION

[399x15]–06]

Report on the Selection of Eligible Countries for Fiscal Year 2016

AGENCY: Millennium Challenge Corporation.

ACTION: Notice.


Dated: December 18, 2015.

Maame Ewusi-Mensah Frimpong,
Vice President and General Counsel, Millennium Challenge Corporation.

Report on the Selection of Eligible Countries for Fiscal Year 2016

Summary
This report is provided in accordance with section 608(d)(1) of the Millennium Challenge Act of 2003, as amended, Public Law 108–199, Division D, the “Act”) (22 U.S.C. 7707(d)(1)).

The Act authorizes the provision of Millennium Challenge Account.