BEFORE THE
UNITED STATES COPYRIGHT OFFICE

Section 512 Study:
Notice and Request for Public Comment
Docket No. 2015-7

Comments on Behalf of Copyright Law Scholars

April 1, 2016

The Honorable Maria A. Pallante
Register of Copyrights
United States Copyright Office
101 Independence Ave., S.E.
Washington, D.C. 20559

Dear Ms. Pallante:

The undersigned copyright law scholars respectfully submit these comments in response to the U.S. Copyright Office's Notice and Request for Public Comment regarding its study of Section 512 of Title 17. These comments were prepared with the assistance of the Arts & Entertainment Advocacy Clinic at George Mason University School of Law.[1]

Our comments are limited to one narrow point:[2] Judicial interpretations of the red flag knowledge standard have disrupted the careful balance of responsibilities that Congress sought to create when it enacted the Digital Millennium Copyright Act. Instead of requiring service providers to take action in the face of red flags, courts have allowed service providers to ignore even the most crimson of flags. Unfortunately, this case law has created an unbalanced atmosphere where service providers are not sufficiently incentivized to work together with copyright owners to develop policies, procedures, and technology to prevent piracy.

We appreciate your leadership on this issue and are thankful for the opportunity to submit these comments.

[1] We would like to thank Mason Law students Danielle Ely and Victor Morales in particular for their hard work in researching and drafting these comments.
[2] We respond to Question 19 of the Notice and Request for Public Comment.

I. Introduction

The Digital Millennium Copyright Act ("DMCA") is not working as Congress intended. Courts have interpreted the red flag knowledge standard to require an exceedingly high level of specific knowledge before service providers risk losing their Section 512 safe harbors. As a result, instead of promoting a system where service providers and copyright owners work together to find and remove infringing materials, Section 512 allows services that provide access to enormous amounts of infringing creative works to avoid liability so long as they properly act on individual takedown notices sent by copyright owners. This one-sided case law has disrupted the careful balance of responsibilities that Congress sought to create when it enacted the DMCA and has made it near-impossible for copyright owners to efficiently prevent large-scale piracy of their works.

II. In enacting the DMCA, Congress intended for service providers and copyright owners to share the burden of preventing online piracy.

Recognizing that "the law must adapt in order to make digital networks safe places to disseminate and exploit copyrighted materials," Congress enacted the DMCA in 1998.[3] The overall intent was to protect innocent service providers that disseminate information online while sustaining the property rights of copyright owners. Congress sought to accomplish this goal by providing "certainty for copyright owners and Internet service providers with respect to copyright infringement liability online."[4] The safe harbors in Section 512 were designed to "ensure[] that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will expand."[5] In particular, Congress intended Section 512 to provide meaningful protections for the exclusive rights of authors while limiting the liabilities of service providers in circumstances that were "widely accepted as fair and reasonable."[6]

In enacting Section 512, Congress sought to "preserve[] 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."[7] Congress well understood the symbiotic relationship between copyright owners and service providers. The online marketplaces made possible by service providers depend upon the creative works of copyright owners to make them thrive. It is only when copyright owners and service providers work together to curb online infringement—both *detecting* and *dealing* with the problem—that Congress's vision for robust, efficient, flexible, and safe online marketplaces can be realized.

Unfortunately, this shared-responsibility approach to respecting and protecting intellectual property rights online has not come to fruition. Instead of service providers and copyright owners working hand-in-hand to nurture safe and legal online marketplaces, courts have interpreted the safe harbor provisions of the DMCA so broadly that service providers have little incentive to pull

[3] S. Rep. No. 105-190, at 2 (1998) [hereinafter "Senate"]; *see also* H.R. Rep. 105-551(I), at 9 (1998) [hereinafter "House I"].
[4] *Id*.; *see also* House I, at 11; H.R. Rep. 105-551(II), at 49 (1998) [hereinafter "House II"].
[5] *Id*.
[6] House I, at 11.
[7] Senate, at 40 (emphasis added); *see also* House II, at 49.

their own weight in detecting and combating online infringement. Since service providers know the red flag knowledge standard is practically insurmountable, they see no reason to work with copyright owners to combat even the most obvious infringements. The result today is that the DMCA is simply not working for copyright owners. While Congress enacted Section 512 to promote cooperation and common sense online, the reality is that it currently does neither.

III. Congress intended Section 512's red flag knowledge standard to eliminate safe harbor protection in cases where the service provider "turn[s] a blind eye to 'red flags' of obvious infringement."

Congress did not create the Section 512 safe harbors in a vacuum. Instead, Congress incorporated then-recent common law developments. Most notably, Section 512 codified Judge Whyte's opinion in *Netcom*, which held that online intermediaries materially contribute to the infringement they enable such that the imposition of contributory liability depends upon their knowledge of the infringement.[8] Accordingly, Section 512(c), which applies to services that provide user storage, and Section 512(d), which applies to services that provide links, condition the availability of the safe harbor on the service provider's knowledge of the infringement.[9]

In order to maintain safe harbor protection under Section 512(c), a service provider must neither "have actual knowledge that the material or an activity using the material on the system or network is infringing" nor be "aware of facts or circumstances from which infringing activity is apparent[.]"[10] This latter standard is referred to as "red flag" knowledge.[11] Once a service provider has either actual or red flag knowledge, it must "act[] expeditiously to remove, or disable access to, the material" in order to keep its safe harbor.[12] The same holds true for service providers under Section 512(d).[13] It is important to note that a service provider can have actual or red flag knowledge even if it has not received a takedown notice from a copyright owner.[14] In fact, Sections 512(c) and (d) both have separate subsections pertaining to service providers that have received a takedown notice.[15]

Under Sections 512(c) and (d), actual knowledge and red flag knowledge are two distinct standards. Importantly, the statutory language clearly denotes a different object for what must be known in order for the service provider to lose the safe harbor:

---

[8] *See* Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1373-75 (N.D. Cal. 1995); *see also* House I, at 11 and 24-25.
[9] *See* 17 U.S.C. §§ 512(c)-(d).
[10] *Id*. at §§ 512(c)(1)(A)(i)-(ii).
[11] *See* Senate, at 44; House I, at 25; House II, at 53.
[12] 17 U.S.C. § 512(c)(1)(A)(iii).
[13] *See* 17 U.S.C. §§ 512(d)(1)(A)-(C); *see also* Senate, at 48; House II, at 57.
[14] *See* Senate, at 45 ("Section 512 does not require use of the notice and take-down procedure. A service provider wishing to benefit from the limitation on liability under subsection (c) must 'take down' or disable access to infringing material residing on its system or network of which it has actual knowledge or that meets the 'red flag' test, even if the copyright owner or its agent does not notify it of a claimed infringement."); House II, at 54.
[15] *See* 17 U.S.C. §§ 512(c)(1)(C) and (d)(3).

- **Actual knowledge –** requires "knowledge that *the* material or an activity using *the* material on the system or network is infringing"[16] or "knowledge that *the* material or activity is infringing"[17]
- **Red flag knowledge** – requires "aware[ness] of facts or circumstances from which infringing activity is apparent"[18]

Thus, the actual knowledge standard requires knowledge that *specific* material ("*the* material") or activity using that *specific* material ("activity using *the* material") is *actually* infringing ("is infringing"), while the red flag knowledge standard requires only *general* awareness ("aware[ness] of facts of circumstances") that activity *appears* to infringe ("is apparent").[19] In Congress's view, the critical distinction between the two knowledge standards was this: Actual knowledge turns on specifics, while red flag knowledge turns on generalities. This is readably discernible from the plain meaning of the statute itself, and it is confirmed explicitly in the legislative history.

Both the Senate and the House Report note that while a service provider has no duty to affirmatively monitor its system for infringement, it loses its safe harbor if it "turn[s] a blind eye to 'red flags' of obvious infringement."[20] The legislative history provides that red flag knowledge has "both a subjective and an objective element."[21] In order for a service provider to have red flag knowledge, it must be subjectively aware of facts or circumstances from which infringing activity would be objectively apparent—that is, the "infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances[.]"[22] Thus, a service provider that knows about obviously-infringing activity *generally*, "in the absence of . . . actual knowledge"[23] that any *specific* material is infringing, would still have red flag knowledge and would need to take action or lose the safe harbor.

The examples given in the legislative history demonstrate Congress's expectation that *general* knowledge of infringing activity could constitute a red flag. For instance:

- A copyright owner could prove that a service provider indexed a site that "was clearly . . . a 'pirate' site . . . where sound recordings, software, movies or books were available for unauthorized downloading, public performance or public display."[24]

---

[16] *Id*. at § 512(c)(1)(A)(i) (emphasis added).
[17] *Id*. at § 512(d)(1)(A) (emphasis added).
[18] *Id*. at §§ 512(c)(1)(A)(ii) and (d)(1)(B)(emphasis added).
[19] *See, e.g.*, 4-12B Nimmer on Copyright § 12B.04[A][1][b][ii] ("To show 'actual knowledge' that disqualifies defendant from the safe harbor, the copyright owner must show that '*the* material' about which complaint is made is infringing. By contrast, to show that a 'red flag' disqualifies defendant from the safe harbor, the copyright owner must simply show that 'infringing activity' is apparent—pointedly, not '*the* infringing activity' alleged in the complaint. In short, the 'actual knowledge' prong is reasonably construed to refer to *specifics*, whereas the 'red flag' prong deals with *generalities*." (emphasis in original; footnotes omitted)).
[20] Senate, at 48; *see also id*., at 44 ("[I]f the service provider becomes aware of a 'red flag' from which infringing activity is apparent, it will lose the limitation of liability if it takes no action."); House I, at 25 ("Once a provider becomes aware of a red flag, however, it ceases to qualify for the exemption."); House II, at 53 and 58.
[21] *Id*., at 44; *see also* House II, at 53.
[22] *Id*.; *see also* House II, at 53.
[23] 17 U.S.C. §§ 512(c)(1)(A)(ii) and (d)(1)(B).
[24] Senate, at 48; *see also* House II, at 57.

- Some sites use slang terms such as "pirate" or "bootleg" that "make their illegal purpose obvious . . . from even a brief and casual viewing" such that "safe harbor status for a provider that views such a site and then establishes a link to it would not be appropriate."[25]

Congress intended for red flag knowledge under Section 512 to "strike[] the right balance" by removing safe harbor protection for service providers that come across something "obviously pirate" and then choose to ignore it.[26] Evidence that service providers were subjectively aware of general indicia such as the examples above could be enough "for copyright owners to rebut their claim to a safe harbor."[27] When a service provider is aware that its service provides access to infringing works and turns a blind eye to that infringing activity, it does so without the benefit of the safe harbors.

Unlike with the actual knowledge standard, Congress did not intend red flag knowledge to require specific knowledge of infringing material. Instead, obvious indicia of infringing activity *generally* should be enough to hoist the red flag. This broad, commonsensical approach is clear from both the statute and the legislative history.

IV. In interpreting the red flag knowledge standard, courts have failed to follow congressional intent.

Unfortunately, courts have severely narrowed the applicability of the red flag knowledge standard, so much so that the distinction between actual and red flag knowledge has been all but lost. In particular, courts have interpreted the red flag knowledge standard to require specific knowledge that so closely matches the actual knowledge standard that it renders red flag knowledge essentially superfluous. This has led to a perverse dynamic where service providers can ignore even widespread, blatant infringement without fear of losing their safe harbor protection. In fact, it incentivizes service providers to do nothing lest they gain actual knowledge and jeopardize their safe harbor protection.

A. *The Ninth Circuit chooses to ignore indicia of infringing activity, contrary to the examples given in the legislative history.*

Courts' confusion in this area has its roots in the Ninth Circuit's *Perfect 10 v. CCBill* decision.[28] Defying congressional intent, the *Perfect 10* court held that even a website providing access to copyrighted works explicitly described as "illegal" or "stolen" was not enough to raise a red flag and eliminate Section 512's safe harbor protection. Regarding the infringing copyrighted works, the court reasoned that the website's description "may be an attempt to increase their salacious appeal, rather than an admission that the [copyrighted works] are actually illegal or stolen."[29]

[25] *Id*.; *see also* House II, at 58.
[26] *Id*., at 49; *see also* House II, at 58.
[27] *Id*., at 48-49; *see also* House II, at 58.
[28] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102 (9th Cir. 2007).
[29] *Id*. at 1114.

Displaying its confusion with the statute, the court emphasized that it reached its holding because "[w]e do not place the burden of determining whether [copyrighted works] are actually illegal on a service provider."[30] This reasoning misses the point of what Congress sought to enact through the red flag knowledge standard. The issue should not have been whether the service provider *subjectively* knew that the material was "actually illegal"—that is the actual knowledge standard. Rather, the issue should have been whether there were enough indicia that the "infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances" such that the service provider at a minimum should have investigated further.[31]

The Court's holding that there were "no such investigative duties"[32] effectively allowed the service provider to avail itself of the safe harbor while turning a blind eye in the face of major red flags. While it's true that service providers generally have no duty to monitor their services or go looking for infringements, the same is not true once they have red flag knowledge that infringing activity is apparent. If they turn a blind eye to such apparent infringing activity, they lose their safe harbor protection. But rather than require the service provider to take action to maintain its safe harbors, the Ninth Circuit let it turn a blind eye and do nothing.

B. *The Second Circuit compounds the problem and the Ninth Circuit doubles down.*

Perhaps the longest nail in the red flag knowledge coffin comes from the Second Circuit's opinion in *Viacom v. YouTube*.[33] In that case, the court held that "the basic operation of § 512(c) requires knowledge or awareness of specific infringing activity."[34] Since a service provider "that gains knowledge or awareness of infringing activity retains safe-harbor protection if it 'acts expeditiously to remove, or disable access to, the material,'" the court reasoned that "the nature of the removal obligation itself contemplates knowledge or awareness of specific infringing material, because expeditious removal is possible only if the service provider knows with particularity which items to remove."[35] The court roundly rejected the argument that the service provider would have "an amorphous obligation to take commercially reasonable steps in response to a generalized awareness of infringement."[36]

Even though employee surveys and financial advisor reports strongly suggested that the service provider was aware that its site provided access to massive quantities of infringing works, the court found that this was insufficient to raise a triable issue of fact regarding red flag knowledge. In the court's view, such claims would be insufficient as a matter of law to demonstrate that the service provider was aware of "specific instances of infringement."[37] This reasoning allows service providers that are *generally* aware of outrageous amounts of infringement to avail themselves of the safe harbor so long as their knowledge is not specific enough to point them to "the existence of particular instances of infringement."[38]

---

[30] *Id*.
[31] Senate, at 44; *see also* House II, at 53.
[32] *Perfect 10*, 488 F.3d at 1114.
[33] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012).
[34] *Id*. at 30.
[35] *Id*. (quoting 17 U.S.C. § 512(c)(1)(A)(iii)).
[36] *Id*. at 30-31 (internal quotations omitted).
[37] *Id*. at 32.
[38] *Id*. at 33.

The problem with the Second Circuit's reasoning is that it is neither compelled by the statute nor consistent with the legislative history. More fundamentally, it rests on the erroneous supposition that a service provider has no duty to investigate further once it becomes "aware of facts or circumstances from which infringing activity is apparent[.]"[39] That is not how Section 512 is supposed to work. It is indeed true that a service provider must, upon obtaining actual or red flag knowledge, "act[] expeditiously to remove, or disable access to, the material[.]"[40] And the Second Circuit was correct to note that with mere red flag knowledge, the service provider would not know which *specific* material to remove. But the obvious answer is this: A service provider with red flag knowledge must investigate further to locate that *specific* material so that it can remove it.

The legislative history makes clear that a service provider loses its safe harbor if it "turn[s] a blind eye to 'red flags' of obvious infringement."[41] The Second Circuit's interpretation, by contrast, allows service providers to simply look the other way even in the face of countless red flags. While Congress intended the safe harbors to reward service providers that work together with copyright owners to combat obvious infringement, the Second Circuit's decision perversely encourages service providers to do nothing and avoid any knowledge of infringement that would be specific enough to allow them to take action.

Making matters worse, the Ninth Circuit in *UMG v. Shelter Capital* adopted the Second Circuit's narrow understanding of the red flag knowledge standard.[42] Despite ample allegations that the service provider was generally aware that it was in fact providing illicit access to numerous copyrighted works, the Ninth Circuit reasoned that the service provider's knowledge was not specific enough to constitute a red flag and that it had no duty to investigate further. Though acknowledging that "a service provider cannot willfully bury its head in the sand,"[43] the Ninth Circuit followed the Second Circuit's lead and nonetheless allowed the service provider to do exactly that.

C. *District courts in other circuits have begun to adopt the Second and Ninth Circuit's reasoning, disrupting the balance of responsibilities that Congress sought to create through Section 512.*

Most copyright cases are brought in the Second and Ninth Circuits, so the erroneous understanding of the red flag knowledge standard in those two circuits has been and will continue to be applied to a large number Section 512 cases. Moreover, the reasoning of the Second and Ninth Circuits is now being extended to district courts in other circuits. For instance, a district court in Florida cited both *Viacom* and *UMG* for the proposition that red flag knowledge requires knowledge of specific infringing material.[44] Likewise, a district court in

[39] 17 U.S.C. §§ 512(c)(1)(A)(ii) and (d)(1)(C).
[40] *Id*. at §§ 512(c)(1)(A)(iii) and (d)(1)(B).
[41] Senate, at 48; *see also id*., at 44 ("[I]f the service provider becomes aware of a 'red flag' from which infringing activity is apparent, it will lose the limitation of liability if it takes no action."); House I, at 25 ("Once a provider becomes aware of a red flag, however, it ceases to qualify for the exemption."); House II, at 53 and 58.
[42] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013).
[43] *Id*.
[44] Disney Enterprises, Inc. v. Hotfile Corp., No. 11-20427-CIV, 2013 WL 6336286, at 27 (S.D. Fla. Sept. 20, 2013).

Colorado cited both cases and held that red flag knowledge under Section 512(c) "does not place upon the service provider the burden of determining whether materials on its system or network are actually illegal."[45]

Despite the clear import of Section 512's broad text and legislative history, courts are extremely reluctant to find red flag knowledge absent highly unusual fact patterns involving direct interactions by service providers with specific, infringing materials.[46] As a result, service providers have little incentive to work together with copyright owners to police and prevent infringement. Beyond complying with takedown notices, service providers effectively have no legal obligation to contribute to the growing struggle to combat piracy, even in cases where their services play a central role in enabling or facilitating piracy. In fact, by turning Congress's legislative intent on its head, courts have created a twisted dynamic where service providers that do less to prevent piracy—and therefore have less specific knowledge of infringement on their services—are less likely to have red flag knowledge and lose their safe harbor.

The perversity of this situation is readily apparent. For example, under a proper interpretation of Section 512, a search engine that indexes hundreds of thousands of links to *The Pirate Bay* would not qualify for safe harbor protection. Congress explicitly stated that the "important intended objective" of Section 512(d) "is to exclude sophisticated 'pirate' directories–which refer Internet users to other selected Internet sites where pirate software, books, movies, and music can be downloaded or transmitted–from the safe harbor."[47] Nonetheless, given the way the courts have interpreted the red flag knowledge standard, search engines today can continue to index hundreds of thousands of links to the site with little concern for liability.

This is not what Congress intended. Congress expected "service providers and copyright owners to cooperate to *detect* and *deal* with copyright infringements that take place in the digital networked environment."[48] Unfortunately, judicial interpretations of Section 512's red flag knowledge standard give service providers no reason to cooperate with copyright owners to detect and prevent the widespread infringement of their creative works. Instead, service providers can simply lie back and wait for copyright owners to tell them about specific instances of infringement, knowing that their only duty is to take down the specific content as notices come in.

V. Conclusion

Congress enacted Section 512 with the purpose of striking a balance between the interests of copyright owners and service providers in the effort to police online copyright infringement. The red flag knowledge standard incorporated into Sections 512(c) and (d) was the cornerstone of a

[45] BWP Media USA Inc. v. Clarity Digital Grp., LLC, No. 14-CV-00467, 2015 WL 1538366, at 9 (D. Colo. Mar. 31, 2015).
[46] For example, in *Columbia Pictures v. Fung*, the Ninth Circuit held that the service provider "had 'red flag' knowledge of a broad range of infringing activity" because the record was "replete" with examples of the service provider encouraging users to infringe "particular copyrighted works[.]" But even here, the level of specificity the court required under the auspices of red flag knowledge would have satisfied the actual knowledge standard. Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020, 1043 (9th Cir. 2013).
[47] Senate, at 48; *see also* House II, at 58.
[48] Senate, at 40 (emphasis added); *see also* House II, at 49.

shared-responsibility approach. Unfortunately, courts have turned this system on its head, permitting service providers to turn a blind eye even in the face of rampant, obvious copyright infringement enabled by their services. This is not what Congress intended. The enormous amount of copyright infringement we see online today is a testament to the problem of courts' interpretation of the red flag knowledge standard.

We thank the Copyright Office for the opportunity to submit these comments.

Respectfully submitted,

Matthew Barblan
Executive Director
Center for the Protection of Intellectual Property
George Mason University School of Law

Devlin Hartline
Assistant Director
Center for the Protection of Intellectual Property
George Mason University School of Law

Sandra Aistars
Clinical Professor
George Mason University School of Law
Senior Scholar and Director of Copyright Research and Policy
Center for the Protection of Intellectual Property

Mark Schultz
Professor of Law
Southern Illinois University School of Law
Co-Founder and Director of Academic Programs
Center for the Protection of Intellectual Property

Adam Mossoff
Professor of Law
George Mason University School of Law
Co-Founder and Director of Academic Programs
Center for the Protection of Intellectual Property

Sean O'Connor
Boeing International Professor of Law
Chair, Center for Advanced Research and Studies on Innovation Policy
University of Washington School of Law

Eric Priest
Professor of Law
University of Oregon School of Law
Senior Scholar
Center for the Protection of Intellectual Property

Kevin Madigan
Research Fellow
Center for the Protection of Intellectual Property
George Mason University School of Law