2016

Three Notice Failures in Copyright Law

Annemarie Bridy
University of Idaho College of Law, abridy@uidaho.edu

PANEL III

THREE NOTICE FAILURES IN COPYRIGHT LAW

ANNEMARIE BRIDY*

This article explores the nature, effects, and means of correcting three instances of notice failure arising from the copyright industries' evolving enforcement efforts in the digital networked environment. The first two instances of notice failure—"red flag" knowledge under the DMCA and ex parte domain name seizures under the PRO-IP Act—involve legislative failures

* Professor of Law, University of Idaho College of Law; Affiliate Scholar, Stanford University Center for Internet and Society (CIS). This article was prepared for the Notice and Notice Failure in Intellectual Property Law Symposium. The author would like to thank Stacey Dogan, Mike Meurer, and the entire IP faculty at Boston University School of Law, as well as the editors of the Boston University Law Review, for the invitation to participate in the Symposium. I owe special thanks to Fred von Lohmann, Lydia Loren, Peter Menell, and Chris Newman for providing helpful comments as the arguments in the article were taking form.

to appreciate the necessity of notice. The third instance of notice failure—injunctions against nonparty online intermediaries in "pirate site" cases—involves judicial failures to appreciate the insufficiency of notice. Each of these notice failures is associated with a different aspect of online copyright enforcement. All three raise fairness issues and increase operating costs and risks for a wide range of online intermediaries, including search engines, cloud storage services, social media platforms, domain name registrars, payment processors, advertising networks, and content delivery networks.

INTRODUCTION

In *Notice Failure and Notice Externalities*, Peter Menell and Michael Meurer explore how notice failures resulting from the fuzzy boundaries of intellectual property entitlements produce negative externalities for developers of new resources, particularly in the information technology sector, where the problem of uncertain patent scope is widely recognized.[1] This article takes a different tack on notice failures and their costs. Shifting focus from resource development to rights enforcement, specifically online anti-piracy enforcement, it considers the nature, effects, and means of correcting three instances of notice failure in copyright law.

The first two instances—"red flag" knowledge under the Digital Millennium Copyright Act[2] ("DMCA") and ex parte domain name seizures under the Prioritizing Resources and Organization for Intellectual Property ("PRO-IP") Act of 2008[3]—involve a legislative failure to appreciate that notice is necessary for the production of predictable and fair legal outcomes. The third instance of notice failure—injunctions against nonparty online intermediaries in civil "pirate site" cases—involves a judicial failure to appreciate that notice alone does not give courts jurisdiction over strangers to the litigation before them.[4] Each of these notice failures is associated with a different aspect of copyright enforcement in the digital environment. All of them create externalities in the form of higher operating costs and increased legal risk for a wide range of online intermediaries, including search engines, cloud storage services, social media platforms, domain name registrars, payment processors, advertising networks, and content delivery networks ("CDNs").

[1] Peter S. Menell & Michael J. Meurer, *Notice Failure and Notice Externalities*, 5 J. LEGAL ANALYSIS 1 (2013); *see also* JAMES BESSEN & MICHAEL J. MEURER, PATENT FAILURE: HOW JUDGES, BUREAUCRATS, AND LAWYERS PUT INNOVATORS AT RISK 8-11 (2008) (comparing real property's efficient notice regime with patent law's inefficient regime and discussing the latter's negative effect on innovation).

[2] Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C.).

[3] Pub. L. No. 110-403, 122 Stat. 4256 (codified as amended in scattered sections of 15, 17, and 18 U.S.C.).

[4] Nonparty injunctions are being issued under Rule 65 of the Federal Rules of Civil Procedure and the All Writs Act. *See infra* Sections III.A and III.B.

I. UNCERTAIN NOTICE: "RED FLAG" KNOWLEDGE UNDER THE DMCA

Early Internet cases reached conflicting conclusions concerning the appropriate rubric under which to analyze the copyright liability of online intermediaries for their users' infringements. Were online intermediaries liable as direct infringers, as the court held in *Playboy Enterprises, Inc. v. Frena*,[5] a 1993 case involving the sharing of copyrighted photos on an electronic bulletin board service ("BBS")?[6] Or were they liable only as secondary infringers, as another court held two years later in *Religious Technology Center v. Netcom On-line Communication Services, Inc.*,[7] a case involving similar facts?[8] As courts across the country grappled with cases of first impression involving copyright liability and online content distribution, Congress recognized that the prospect of unlimited legal exposure for Internet intermediaries threatened to stifle both innovation in online services and investment in network infrastructure.[9] In light of the dynamic state of affairs in the courts, Congress enacted the safe harbors in Title II of the DMCA to create a cooperative enforcement regime between rights holders and service providers that would give service providers the certainty they needed to grow their platforms.[10]

The safe harbors give service providers relief from monetary damages for claims of direct and secondary copyright infringement.[11] In return, service providers must assist rights holders with online enforcement by removing illegal copyrighted content from their systems when they learn about it.[12] It

[5] 839 F. Supp. 1552 (M.D. Fla. 1993).

[6] *See id.* at 1559 (holding that the defendant BBS operator was liable for direct infringement of the public display and distribution rights of the plaintiff).

[7] 907 F. Supp. 1361 (N.D. Cal. 1995).

[8] *See id.* at 1369, 1373 (holding that the defendant Internet access provider was not liable for direct infringement, but was potentially liable for contributory and vicarious infringement).

[9] *See* S. REP. NO. 105-190, at 8 (1998) ("[W]ithout clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet. . . . [B]y limiting the liability of service providers, the DMCA ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand.").

[10] *See* H.R. REP. NO. 105-551, pt. 2, at 49-50 (1998) ("[Title II] provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities."); S. REP. NO. 105-190, at 2 ("Title II will provide certainty for copyright owners and Internet service providers with respect to copyright infringement liability online.").

[11] *See* S. REP. NO. 105-190, at 40 ("The limitations in subsections (a) through (d) protect qualifying service providers from liability for all monetary relief for direct, vicarious and contributory infringement.").

[12] 17 U.S.C. § 512(c)(1)(A) (2012) (stating that a service provider will not be liable for storage of infringing material on its system if the service provider "acts expeditiously to remove, or disable access to, the material" upon acquiring knowledge or awareness of its existence); *id.* § 512(c)(1)(C) (stating that a service provider will not be liable for storage of

sounds like a simple bargain, but the devil is in the details, of which there are very, very many.[13] Almost twenty years after the DMCA's passage, rights holders and online intermediaries continue to fight costly and protracted legal battles focused on the scope of the safe harbors and what conditions service providers must fulfill to come within them.[14] Almost inevitably, these disputes concern contributory infringement and the question of how and when a service provider acquires actionable knowledge of infringement.[15] Entangled with that question is another: What kind of notice can confer actionable knowledge under the statute? Normatively speaking, the answer to the notice question should be relatively transparent, given that the safe harbors exist to provide legal certainty for intermediaries concerning their exposure to copyright infringement claims. Unfortunately, that's not the case.[16] And therein lies the first notice failure this article will discuss.[17]

infringing material on its system if the service provider "upon notification . . . responds expeditiously to remove, or disable access to, the material that is claimed to be infringing").

[13] *See* JESSICA LITMAN, DIGITAL COPYRIGHT 122-50 (2006) (describing, in minute detail, the behind-the-scenes horse trading that produced a bill nearly fifty pages and thirty thousand words long).

[14] *See, e.g.*, Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020, 1024 (9th Cir. 2013) (affirming the district court's grant of summary judgment for Columbia Pictures based on the safe harbor ineligibility of the torrent trackers isoHunt, Torrentbox, and Podtropolis); UMG Recordings, Inc. v. Shelter Capital Partners LLC (*Veoh III*), 718 F.3d 1006, 1036 (9th Cir. 2013) (affirming the district court's grant of summary judgment for the video-sharing service Veoh based on its safe harbor eligibility); Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 25-26 (2d Cir. 2012) (deciding an appeal of a grant of summary judgment for the video-sharing service YouTube on the question of its safe harbor eligibility); Capitol Records, LLC v. Vimeo, LLC, 972 F. Supp. 2d 537, 556 (S.D.N.Y. 2013), *appeal docketed*, No. 14-1048 (2d Cir. Apr. 9, 2014) (deciding a motion for reconsideration by the video-sharing service Vimeo on the question of its safe harbor eligibility and certifying for interlocutory appeal two questions concerning the scope of the safe harbors).

[15] Knowledge is an element of the prima facie case for contributory copyright infringement. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1020 (9th Cir. 2001) ("Contributory liability requires that the secondary infringer 'know or have reason to know' of direct infringement.").

[16] Jessica Litman has characterized the safe harbors as "an opportunity [for Internet service providers] to jump through a long, complicated series of hoops and thereby avoid liability." LITMAN, *supra* note 13, at 143. Her critique is reminiscent of Larry Lessig's characterization of fair use as "the right to hire a lawyer." LAWRENCE LESSIG, FREE CULTURE 187 (2004).

[17] Peter Menell and Michael Meurer have explored notice failure and its externalities in the context of the development and claiming of intellectual property. *See* Menell & Meurer, *supra* note 1. They define "notice information" as "ownership/boundary facts as well as legal standards governing the scope of property rights." *Id.* at 5.

A. *As Clear As Day: Notifications of Claimed Infringement*

The DMCA's well-known notice-and-takedown protocol is at the heart of the safe harbors. The protocol requires a qualifying service provider to promptly remove or disable access to copyrighted content on its system after receiving a "notification of claimed infringement" from a rights holder concerning that content.[18] Section 512(c)(3)(A) of the statute prescribes in detail the elements of an effective notification.[19] It must be a written communication, directed to the service provider's designated DMCA agent, that includes "substantially" (1) a physical or electronic signature of the authorized sender; (2) identification of the allegedly infringed work or a representative list of such works if the notice covers more than one; (3) identification of the allegedly infringing material online and information sufficient to allow the provider to locate it; (4) physical and electronic contact information for the complainant; (5) a statement that the complainant has a good faith belief that the material is being used illegally; and (6) a statement, under penalty of perjury, that the complainant is authorized to act for the rights holder of the allegedly infringed work.[20]

The statute is equally specific about the consequences of sending (and receiving) a non-compliant notification; such a notification "shall not be considered" when determining whether a service provider has the requisite knowledge to trigger its duty to remove content in order to avoid liability.[21] There is some wiggle room for rights holders who fail to meet all of the formalities of notification. If the notification substantially identifies the allegedly infringed work or works, identifies the online location information for the allegedly infringing material, and provides contact information for the complainant, then the provider must promptly attempt to contact the complainant or "take[] other reasonable steps to assist in the receipt of [a substantially compliant] notification."[22] By identifying the most important elements of a notification and providing clear direction to providers who receive defective but recuperable notifications, the statute retains certainty without elevating form over substance to the detriment of aggrieved rights holders.[23] Although the safe harbor case law is peppered with disputes over the

[18] *See* 17 U.S.C. § 512(c)(1)(C) (2012).

[19] *Id*. § 512(c)(3)(A) (detailing the six elements of an effective notification).

[20] *Id*. § 512(c)(3)(A)(i)-(vi).

[21] *Id*. § 512(c)(3)(B)(i).

[22] *Id*. § 512(c)(3)(B)(ii).

[23] *Cf*. H.R. REP. NO. 105-551, pt. 2, at 56 (1998) ("[T]echnical errors (e.g., misspelling a name, supplying an outdated area code if the phone number is accompanied by an accurate address, supplying an outdated name if accompanied by an e-mail address that remains valid for the successor of the prior designated agent or agent of a copyright owner) do not disqualify service providers and copyright owners from the [DMCA's safe harbor] protections . . . .").

adequacy of purported takedown notifications, the issue has not been highly controversial in the courts in light of the clear guidance the statute provides.[24]

A potentially significant notice-related uncertainty in § 512(c)(3)(A) does arise from the language permitting a complaining rights holder to submit a "representative list" of infringed works in a single notification.[25] That provision could be interpreted to imply an obligation on a service provider's part to search its service for material that is potentially infringing but is *not* itemized on a rights holder's notification—an obligation that would run counter to § 512(m) of the statute, which absolves service providers of any affirmative duty to investigate or monitor their services for infringing activity.[26] One court finessed the tension between these two sections of the statute by holding that any works not specifically identified in a notification must be easily identifiable as the complainant's property (e.g., through the appearance of an attached copyright notice naming the complainant as the rights holder) and located at a URL or URLs expressly specified by the rights holder in the notification.[27]

Courts have also limited the "representative list" provision by emphasizing that the statute on its face requires a list of copyrighted *works* and not, as some plaintiffs have asserted, a list of recording artists to whom dozens or even hundreds of unspecified works could be attributed.[28] A more permissive

[24] *See, e.g.*, Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1113 (9th Cir. 2007) (affirming summary judgment for the defendant service provider on the issue of safe harbor qualification, and stating that it would unduly burden service providers to permit a plaintiff to "cobble together adequate notice from separately defective notices"); Hendrickson v. eBay Inc., 165 F. Supp. 2d 1082, 1089, 1092 (C.D. Cal. 2001) (granting summary judgment to eBay on the issue of safe harbor eligibility because, inter alia, a "pre-suit 'cease and desist' letter and e-mails to eBay [did] not include several of the key elements for proper notice required by Section 513(c)(3)" and were therefore not effective to confer actionable knowledge on the defendant).

[25] 17 U.S.C. § 512(c)(3)(A)(ii).

[26] *See id.* § 512(m) ("Nothing in this section shall be construed to condition [safe harbor eligibility] on—(1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity . . . .").

[27] *See* ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619, 625 (4th Cir. 2001) ("ALS Scan provided RemarQ with information that (1) identified two sites created for the sole purpose of publishing ALS Scan's copyrighted works, (2) asserted that virtually all the images at the two sites were its copyrighted material, and (3) referred RemarQ to two web addresses where RemarQ could find pictures of ALS Scan's models and obtain ALS Scan's copyright information. In addition, it noted that material at the site could be identified as ALS Scan's material because the material included ALS Scan's 'name and/or copyright symbol next to it.' We believe that with this information, ALS Scan substantially complied with the notification requirement of providing a representative list of infringing material as well as information reasonably sufficient to enable RemarQ to locate the infringing material.").

[28] *See* UMG Recordings, Inc. v. Veoh Networks Inc. (*Veoh I*), 665 F. Supp. 2d 1099, 1110 (C.D. Cal. 2009), *aff'd on reh'g sub nom.* UMG Recordings, Inc. v. Shelter Capital

reading would undermine the DMCA's lynchpin principle that a notification is substantially compliant only if it contains sufficient information for a provider to locate specific infringing files on its site.[29] Without adequate location information from a complaining rights holder, a provider is unable to fulfill its statutory duty to remove content unless it undertakes the kind of investigation that § 512(m) expressly excuses providers from having to undertake.[30]

The notice-and-takedown protocol is straightforward and highly prescriptive by design; a rights holder's substantially compliant notification triggers a service provider's obligation to remove content, and the service provider's prompt removal of the specified content secures the protection of the safe harbor. The statute states in detail what counts as a compliant notification, and it expressly sets forth the legal-epistemic consequences of a service provider's failing to receive such a notification. Simply put, a materially defective notification does not confer guilty, actionable knowledge on a service provider.[31] When defining the safe harbors, Congress wanted to draw bright lines on which intermediaries and their investors could rely, even in the face of evolving liability rules. With respect to the question of what constitutes a substantially compliant notification under § 513(c)(3)(A), Congress succeeded in that goal.

B. *As Clear As Mud: Red Flags of Infringement*

A substantially compliant notification is not the only trigger, however, for a service provider's duty to remove content if it wants safe harbor protection under the DMCA. The duty is also triggered by so-called "red flag" knowledge, defined in § 512(c)(1)(A) of the statute as "aware[ness] of facts or circumstances from which infringing activity is apparent."[32] Under the DMCA, both sources of notice can operate to deprive a service provider of safe harbor. But whereas the requirements for a compliant notification are clear on the face of the statute, the precise contours of red flag knowledge continue to elude

Partners LLC (*Veoh III*), 718 F.3d 1006 (9th Cir. 2013) ("What the RIAA did—*i.e.*, provide names of *artists*—and what the statute requires—*i.e.*, a representative list of *works*—are not quite the same."); Arista Records, Inc. v. MP3Board, Inc., No. 00 CIV. 4660(SHS), 2002 WL 1997918, at *9 (S.D.N.Y. Aug. 29, 2002) ("The citation to a handful of performers does not constitute a representative list of infringing material, and certainly did not provide information reasonably sufficient to enable MP3Board to locate the particular infringing works.").

[29] *See* Viacom Int'l Inc. v. YouTube, Inc. (*YouTube I*), 718 F. Supp. 2d 514, 528-29 (S.D.N.Y. 2010), *aff'd in part, vacated in part*, 676 F.3d 19 (2d Cir. 2012) ("This 'representative list' reference would eviscerate the required specificity of notice . . . if it were construed to mean a merely generic description ('all works by Gershwin') without also giving the works' locations at the site, and would put the provider to the factual search forbidden by § 512(m).").

[30] *See id*.

[31] *See* 17 U.S.C. § 512(c)(3).

[32] *Id*. § 512(c)(1)(A)(ii).

litigants and courts. By muddying the statute's otherwise clear rules about notification with the ambiguous standard of red flag notice, Congress codified a notice failure in the DMCA that deprives online intermediaries of the predictability the law was intended to afford.[33] John Blevins has argued persuasively that rights holders have leveraged the uncertainty inherent in the red flag standard to raise the costs of enforcement-related litigation for online intermediaries and to create incentives for them to become proactive co-enforcers.[34]

The case law concerning the scope of red flag knowledge is not altogether lacking in clarity. The cases do coalesce on the principle that red flag knowledge must be item-specific; it is not a generalized knowledge of infringement that follows inexorably either from the knowledge that a service *can* be used to infringe or from knowledge that a service provider gains from receiving compliant notifications under § 512(c)(3)(A).[35] The cases also establish that red flag knowledge incorporates both a subjective and an objective element: "[T]he red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement 'objectively' obvious to a reasonable person."[36] Beyond these two points of agreement, however, the decisional law gets very muddy very quickly, notwithstanding a legislative history that treats questions surrounding red flags as cut and dried. The legislative history of the DMCA contemplates that the red flag provision should have a very narrow application, justifying imputation of knowledge to a provider only in cases involving "obvious and conspicuous circumstances," such as where a site is completely dedicated to infringing content and operates with no discernable lawful purpose.[37]

In retrospect, the provision's reach has not been so easy to cabin. Where rights holders see unrepentant bad actors,[38] others see legitimate businesses

[33] *See supra* note 10 and accompanying text.

[34] John Blevins, *Uncertainty as Enforcement Mechanism: The New Expansion of Secondary Copyright Liability to Internet Platforms*, 34 CARDOZO L. REV. 1821, 1824 (2013) ("In short, uncertainty 'outsources' enforcement costs to Internet platforms.").

[35] *See Veoh III*, 718 F.3d 1006, 1023 (9th Cir. 2013) ("[A provider's] general knowledge that it hosted copyrightable material and that its services could be used for infringement is insufficient to constitute a red flag."); Viacom Int'l, Inc. v. YouTube, Inc. (*YouTube II*), 676 F.3d 19, 32 (2d Cir. 2012) (defining red flag knowledge as "awareness of facts or circumstances that indicate *specific and identifiable instances* of infringement" (emphasis added)).

[36] *YouTube II*, 676 F.3d at 31.

[37] S. REP. NO. 105-190, at 49 (1998).

[38] *Cf.* Stuart Dredge, *BPI: 'Google Leads Consumers into a Murky Underworld of Unlicensed Sites,'* MUSIC ALLY (Nov. 15, 2013), http://musically.com/2013/11/15/bpi-google-leads-consumers-into-a-murky-underworld-of-unlicensed-sites/ [https://perma.cc/54JB-K5SA] (reporting on the music industry's sharp criticism of Google's anti-piracy efforts related to online search results); Richard Verrier, *MPAA Report Says Google, Other Search Engines a Major Gateway to Piracy*, L.A. TIMES (Sept. 18, 2013, 7:36 AM),

with copyright-intensive operating models—businesses the safe harbors were explicitly designed to protect. By invoking the red flag provision against popular service providers that they believe are not sufficiently aggressive (read: proactive) in their enforcement efforts, rights holders have tried indirectly to chip away at § 512(m)'s no-duty-to-monitor rule.[39]

The music industry's suit against video-hosting platform Veoh is a good example of this strategy. Universal Music Group ("UMG") litigated Veoh into bankruptcy[40] over the red flag question, arguing—ultimately unsuccessfully—that Veoh should be disqualified from the safe harbor because it failed to show "initiative" by not implementing "search and indexing tools to locate and remove" all files belonging to artists previously identified in the Recording Industry Association of America's ("RIAA") § 512(c)(3)(A) notifications.[41] The underlying logic of UMG's argument was that a § 513(c)(3)(A) notification concerning a specific work by an artist ipso facto creates red flag knowledge of any other works by the same artist that may exist on the service.[42] A provider's failure to find and remove such other works, UMG urged the court to hold, should deprive that provider of safe harbor.[43] The court was unwilling to accept such a broad reading of the red flag provision, which would have amounted to a judicial repeal of § 512(m).[44]

---

http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-mpaa-piracy-study-20130918-story.html [https://perma.cc/EF8Z-ZHA5] (reporting on the motion picture industry's criticism of Google).

[39] *See, e.g.*, Capitol Records, LLC v. Escape Media Grp., Inc., No. 12-CV-6646 (AJN), 2015 WL 1402049, at *57 (S.D.N.Y. Mar. 25, 2015) (recognizing the tension between the doctrine of red flag knowledge and § 512(m)'s rule that providers have no duty to affirmatively police their services for infringing activity); Square Ring, Inc. v. Doe-1, No. 09-563 (GMS), 2015 WL 307840, at *1, *6 (D. Del. Jan. 23, 2015) (accepting the plaintiff's argument that the operator of a streaming video site might be chargeable with red flag knowledge for failing to respond to non-compliant takedown notices sent *in advance of* an anticipated infringement and demanding that the provider proactively block the anticipated infringement); Arista Records LLC v. Myxer Inc., No. CV 08-03935-GAF, 2011 WL 11660773, at *26-27 (C.D. Cal. Apr. 1, 2011) (rejecting the plaintiff's argument that the defendant should be charged with red flag knowledge or willful blindness to red flags because it failed to implement a digital fingerprinting system that blocks user uploads when they match copyrighted reference files in the system's database).

[40] *See* Chloe Albanesius, *Veoh Co-Founder Confirms Bankruptcy*, PCMAG (Feb. 12, 2010, 9:36 AM), http://www.pcmag.com/article2/0,2817,2359105,00.asp [https://perma.cc/362L-NWB7] ("The co-founder of video Web site Veoh confirmed Wednesday night that the recession and legal troubles have prompted the site to file for bankruptcy.").

[41] *Veoh III*, 718 F.3d 1006, 1023-24 (9th Cir. 2013).

[42] *See id.*

[43] *See id.*

[44] *See id.* ("As we have explained, however, to so require would conflict with § 512(m) . . . .").

Just as the red flag provision was not intended to impose an affirmative monitoring obligation on service providers, it was not intended to require service providers to make judgment calls about possible infringements.[45] That is what the red flag provision requires in practice, however, insofar as it creates an amorphous form of notice (and a corresponding removal obligation) that operates entirely outside the clearer parameters of § 512(c)(3)'s notice-and-takedown protocol.[46] The DMCA's red flag provision is the notice exception that swallows the notice rule, requiring minute examination of specific facts to determine whether an accused service provider ignored "objectively obvious" individual infringements.[47]

The multimillion dollar question with red flag notice is what makes an infringement "objectively obvious." Because the applicable standard is obviousness to a reasonable person, the issue is by and large not amenable to disposition on summary judgment.[48] For example, rights holders have argued that high production values in uploaded content should be regarded as a per se

[45] S. REP. NO. 105-190, at 49 (1998).

[46] *See* sources cited *supra* note 39.

[47] *See, e.g.*, Disney Enters., Inc. v. Hotfile Corp., No. 11-20427-CIV, 2013 WL 6336286, at *28 (S.D. Fla. Sept. 20, 2013) ("[T]o the extent that communications with users should have alerted Hotfile to the infringing nature of files on its system that were owned by the Studios . . . , Hotfile might be deemed to have possessed red flag knowledge."); Capitol Records, LLC v. Vimeo, LLC, 972 F. Supp. 2d 500, 521-22 (S.D.N.Y. 2013) ("Plaintiffs claim that Vimeo employees' interactions with these fifty-five Videos-in-Suit necessitates a determination that Vimeo had actual or red flag knowledge of the videos' infringing content. The Court disagrees. . . . Rather, the Court finds that a triable issue remains as to whether . . . this standard is met as to each of the fifty-five videos in question."); Capitol Records, Inc. v. MP3tunes, LLC, No. 07 Civ. 9931(WHP), 2013 WL 1987225, at *4 (S.D.N.Y. May 14, 2013) ("Since something less than a formal takedown notice may now establish red flag knowledge . . . , the issue of Defendants' red flag knowledge cannot be resolved on summary judgment."). For a survey of the red flag cases, see Methaya Sirichit, *Catching the Conscience: An Analysis of the Knowledge Theory Under § 512(c)'s Safe Harbor & the Role of Willful Blindness in the Finding of Red Flags*, 23 ALB. L.J. SCI. & TECH. 85 (2013). Further muddying the waters of § 512 is the Second Circuit's holding in *Viacom International, Inc. v. YouTube, Inc.* that the common law doctrine of willful blindness represents a third, non-abrogated source of knowledge under the DMCA. 676 F.3d at 35. A discussion of the willful blindness doctrine and its relationship to both the red flag provision and the no-duty-to-monitor provision is beyond the scope of this project. Willful blindness doctrine is a notice failure in its own right, however, for the same reasons that the red flag provision is a notice failure.

[48] *See In re* Software Toolworks Inc., 50 F.3d 615, 621 (9th Cir. 1994) ("[S]ummary judgment is generally an inappropriate way to decide questions of reasonableness because 'the jury's unique competence in applying the "reasonable man" standard is thought ordinarily to preclude summary judgment.'" (quoting TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 450 n.12 (1976)); Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 180 (7th Cir. 1991) ("[W]hat is reasonable is itself a fact for purposes of Rule 56 of the civil rules.").

red flag of infringement.[49] But courts have pointed out that the general public has affordable access in today's market to high-quality recording and editing equipment, so that there is often little or no perceptible distinction between amateur and professional content.[50] Further complicating the question of objective obviousness is the fact that users who upload copyrighted content without authorization are entitled to a limited range of unauthorized but fair uses.[51] Requiring service providers to engage in intensive factual inquiries like the one required to determine fair use is exactly what the DMCA was supposed to avoid.

To relieve service providers from having to make judgments about fair use, the notice-and-takedown framework incorporates a "counter-notification" provision, which allows users to request automatic restoration of material that has been removed in response to DMCA notifications if they believe their use of the material is fair or otherwise lawful.[52] Under the counter-notification provision, the service provider is insulated from liability for any material it restores at a user's request.[53] If the rights holder disputes the user's claim of fair use, its remedy under the DMCA is to file suit in federal court against the user, taking the service provider out of the middle.[54]

Operating within the notice-and-takedown framework, a service provider is never put in the position of having to form a legal conclusion about the copyright or fair-use status of user-generated content, and a user whose material is removed in response to a takedown notification gets an opportunity to contest it. The provider is not liable to a user when it removes material in response to a rights holder's compliant notification, and it is not liable to a rights holder when it restores removed material in response to a user's

[49] Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1149 (N.D. Cal. 2008) (rejecting the plaintiff's argument that "the professionally created nature of submitted content constitutes a per se 'red flag' of infringement sufficient to impute the requisite level of knowledge or awareness to Veoh"); *cf.* Mavrix Photographs LLC v. LiveJournal, Inc., No. SACV 13-00517-CJC(JPRx), 2014 WL 6450094, at *6 (S.D. Cal. Sept. 19, 2014) ("Mavrix contends that LiveJournal knew the photographs were 'likely somebody else's copyrighted property . . . since this type of material is frequently shot by professional paparazzi photographers . . . .'").

[50] *Io*, 586 F. Supp. 2d at 1149; *see also Mavrix*, 2014 WL 6450094, at *6 ("[I]t would be nearly impossible for a provider to distinguish between 'professional paparazzi' photographs, which Mavrix contends would be objectively obvious infringing content, and photographs taken by any member of the public with a digital camera or smartphone.").

[51] *See* 17 U.S.C. § 107 (2012).

[52] *See id.* § 512(g) (setting forth procedures for counter-notification and restoration of claimed infringing material).

[53] *Id.* (stating that the service provider is not liable for restoring material at a user's request if the rights holder who submitted the original takedown notice fails to take action after learning about the counter-notification).

[54] *Id.*

compliant counter-notification.[55] The DMCA's protections for users are limited, however, to removals in response to takedown notifications; user protections are not triggered when service providers remove material based on what they believe to be actionable red flags.[56] Removal of user-generated content outside the notice-and-takedown framework thus deprives users of the notice to which *they* are entitled under the DMCA when a service provider removes content in response to a § 512(c)(3)(A) notification.[57] Red flag removals thus short circuit the counter-notification and restoration provisions of the framework, thereby upsetting the checks and balances protecting users' freedom of expression.[58]

Predictably, the legal outcomes of fact-sensitive inquiries about the obviousness of infringement fall all over the map, adding uncertainty to inefficiency.[59] The convoluted procedural histories of the two leading cases on red flags, *Viacom International, Inc. v. YouTube, Inc.*[60] in the Second Circuit, and *UMG Recordings, Inc. v. Shelter Capital Partners LLC*[61] in the Ninth Circuit, illustrate how difficult it has been for courts to apply the red flag standard, and to determine which questions concerning red flags can be decided as a matter of law and which must go to a jury. Viacom sued YouTube in New York in 2007.[62] The case finally settled, with its second appeal

[55] *Id.*; *see also id.* § 512(g)(3) (detailing the requirements for a compliant counter-notification); *supra* note 53 and accompanying text.

[56] 17 U.S.C. § 512(g)(1)-(2).

[57] *See id.* § 512(g)(2) (requiring the service provider, following receipt of a compliant notification, to "take[] reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material").

[58] *See* S. REP. NO. 105-190, at 50 (1998) ("The put back procedures were added . . . to address . . . concerns . . . that other provisions of this title established strong incentives for service providers to take down material, but insufficient protections for third parties whose material would be taken down.").

[59] *Compare, e.g.*, Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020, 1043 (9th Cir. 2013) (finding red flag knowledge as a matter of law where "[t]he material in question was sufficiently current and well-known" that its copyrighted and unlicensed status would have been objectively obvious to a reasonable person), *with* Capitol Records, LLC v. Vimeo, LLC, 972 F. Supp. 2d 500, 522 (S.D.N.Y. 2013) (declining to find red flag knowledge as a matter of law where the defendant's employees interacted with material that "would be characterized by many as popular, and in some cases legendary").

[60] *YouTube I*, 718 F. Supp. 2d 514, 528-29 (S.D.N.Y. 2010), *aff'd in part, vacated in part*, 676 F.3d 19 (2d Cir. 2012), *remanded to* 940 F. Supp. 2d 110, 113 (S.D.N.Y. 2013).

[61] *See Veoh I*, 665 F. Supp. 2d 1099, 1110 (C.D. Cal. 2009), *aff'd sub nom.* UMG Recordings, Inc. v. Shelter Capital Partners LLC (*Veoh II*), 667 F.3d 1022 (9th Cir. 2011), *withdrawn, and aff'd on reh'g*, 718 F.3d 1006 (9th Cir. 2013).

[62] Jonathan Stempel, *Google, Viacom Settle Landmark YouTube Lawsuit*, REUTERS (Mar. 18, 2014, 11:13 AM), http://www.reuters.com/article/us-google-viacom-lawsuit-idUSBREA2H11220140318 [https://perma.cc/AZ7H-QTD5].

pending, in 2014—seven years and three judicial opinions later.[63] UMG sued Veoh in California, also in 2007.[64] Following a grant of summary judgment for Veoh in 2009,[65] the Ninth Circuit affirmed in 2011.[66] The panel later withdrew its opinion for reconsideration following the Second Circuit's decision in the first *YouTube* appeal.[67] The Ninth Circuit issued its second (and final) opinion in *Veoh*, another affirmance, in 2013.[68] Veoh closed shop in 2010, however, long before it could savor victory.[69] For anyone not keeping track, that's two cases, two circuits, eight judges, six opinions, one bankruptcy, seven years of litigation, and far too many lawyers and amici to count. So much for certainty.

The uncertain legal environment that the red flag provision has created negatively impacts the business environment for service providers, particularly for new entrants.[70] When Viacom sued YouTube, seeking $1 billion in statutory damages, YouTube had recently been acquired by Google for stock valued at $1.65 billion.[71] Viacom's suit, in other words, laid claim to sixty percent of YouTube's value as a company. A reporter for Forbes described the case as "a lawyer's dream—and a shareholder's nightmare."[72] Year after year, Google cites the potential for copyright liability and high damage awards as a

[63] *Id*.

[64] *Veoh I*, 665 F. Supp. 2d at 1100. Only months before, Veoh had sued UMG for a declaratory judgment. *See* Veoh Networks, Inc. v. UMG Recordings, Inc., 522 F. Supp. 2d 1265, 1267 (S.D. Cal. 2007) (dismissing Veoh's declaratory judgment action as premature); Richard Koman, *Video Site Veoh Sues to Stop Universal*, NEWSFACTOR (Aug. 10, 2007), http://www.newsfactor.com/story.xhtml?story_id=13300C819SYD [https://perma.cc/ZBC5-5JED].

[65] *Veoh I*, 665 F. Supp. 2d at 1101, 1118 (granting Veoh's motion for summary judgment based on its eligibility for § 512(c)'s safe harbor).

[66] *Veoh II*, 667 F.3d 1022, 1026 (9th Cir. 2011), *withdrawn and superseded on reh'g*, 718 F.3d 1006 (9th Cir. 2013).

[67] 1 IAN C. BALLON, E-COMMERCE & INTERNET LAW § 4.12[6][D] (2d ed. 2015).

[68] *Veoh III*, 718 F.3d at 1011.

[69] Sumner Lemon, *Video Site Veoh Bankrupt, Heads into Liquidation*, COMPUTERWORLD (Feb. 12, 2010, 1:26 AM), http://www.computerworld.com/article/2520881/it-careers/video-site-veoh-bankrupt--heads-into-liquidation.html [https://perma.cc/4JFJ-PEX9].

[70] *See* Eric Goldman, *How the DMCA's Online Copyright Safe Harbor Failed*, 3 NAT'L TAIPEI U. TECH. J. INTELL. PROP. L. & MGMT. 195, 198 (2014) (asserting that the DMCA's ambiguous knowledge standard, along with other factors, "substantially raises the amount of cash required to enter the user-generated content business, as a portion (effectively, the first funds raised) must be set aside for the seemingly inevitable and quite expensive ligation that will surely ensue"); *cf*. LESSIG, *supra* note 16, at 191 ("It is hard enough to start a company. It is impossibly hard if that company is constantly threatened by litigation.").

[71] *See* Lisa Lerer, *Viacom's Expensive Suit*, FORBES (Mar. 28, 2007, 6:00 AM), http://www.forbes.com/2007/03/27/youtube-viacom-google-tech-cx_ll_0328google.html [https://perma.cc/4AAA-297W]; Andrew Ross Sorkin & Jeremy W. Peters, *Google to Acquire YouTube for $1.65 Billion*, N.Y. TIMES (Oct. 9, 2006), http://www.nytimes.com/2006/10/09/business/09cnd-deal.html?_r=0 [https://perma.cc/XLZ8-3JNU].

[72] Lerer, *supra* note 71.

risk factor in its SEC filings.[73] Thanks to Google's deep pockets, YouTube was in a financial position to weather the storm of protracted litigation over the question of its safe harbor eligibility[74]—a question that had still not been definitively answered when the case settled. Veoh was not so lucky in the start-up sweepstakes; the pending litigation with UMG chilled potential investors and prevented the company from raising capital at a critical juncture.[75] Veoh thus became a casualty of the notice failure inherent in the DMCA safe harbors and an example of how the safe harbors have failed to provide a predictable, navigable legal environment for Internet start-ups.[76]

C. *Fixing the Failure: DMCA Reform and the Future of Red Flags*

It is no profound insight to realize that the DMCA's red flag provision is an instance of notice failure in copyright law; anyone passingly familiar with the statute and the litigation it has spawned can see it. Indeed, the people in government whose job it is to think about these things have their eye on the ball. As part of a comprehensive review of existing Internet policy, the Department of Commerce published a green paper on copyright in 2013.[77] In the green paper, the Department's Internet Policy Task Force identified ambiguities in the DMCA's knowledge standard as an issue in need of resolution, but the authors seemed satisfied that the courts will stabilize the doctrine over time.[78] Accordingly, the Task Force did not recommend any legislative action relating to the safe harbors.

The Register of Copyrights, Maria Pallante, has been less optimistic about the judiciary's ability to correctly interpret and apply the safe harbors. In a 2013 lecture summarizing problems the "Next Great Copyright Act" should solve, Pallante noted that the § 512 safe harbors "have generated more than their fair share of litigation," particularly on the issues of eligibility and

[73] *See, e.g.*, Google Inc., Annual Report (Form 10-K) 10-11 (Feb. 11, 2016) [hereinafter Google 10-K] ("We are, and may in the future be, subject to intellectual property or other claims, which are costly to defend, could result in significant damage awards, and could limit our ability to use certain technologies in the future.").

[74] *See* Lerer, *supra* note 71 (estimating that Google and Viacom's legal fees in the case could reach over $350 million).

[75] *See* Lemon, *supra* note 69 ("Dmitry Shapiro, Veoh's founder and CEO, blamed the company's collapse on a costly legal battle with Universal Music Group, which Veoh ultimately won, and a difficult economic environment.").

[76] *Cf.* Google 10-K, *supra* note 73, at 9 (identifying as a risk factor the fact that "laws relating to the liability of providers of online services are currently unsettled both within the U.S. and abroad").

[77] INTERNET POLICY TASK FORCE, DEP'T OF COMMERCE, COPYRIGHT POLICY, CREATIVITY, AND INNOVATION IN THE DIGITAL ECONOMY (2013).

[78] *See id.* at 54-55 ("Resolution of these questions by the courts will provide greater certainty to both right holders and [Internet service providers] and enable a clearer understanding of whether the safe harbors are operating as intended.").

monitoring.[79] Revisiting the topic in congressional testimony in 2015, she expressed doubt about the soundness of the evolving judicial consensus on red flag knowledge, i.e., that the red flag provision must be construed narrowly to preserve the allocation of enforcement burdens that Congress intended.[80] Citing *Veoh* and *YouTube* as examples of judicial interpretations that "some believe run counter to the very balance that the DMCA sought to achieve," Pallante called for a formal study of § 512 "to consider what is working and what is not, along with potential legislative improvements."[81]

Legislative improvements, like beauty, are in the eye of the beholder. In keeping with that axiom, it is unlikely that rights holders and service providers will ever agree on how to fix the notice failure they can readily agree is embodied in the red flag provision. The sticking point is ultimately economic; each side wants the other to shoulder the lion's share of enforcement costs, which can be substantial given the scale at which infringement occurs on services eligible for safe harbor. For large, well-capitalized providers like the Googles and Facebooks of the world, taking on extra enforcement burdens may not be onerous. For new entrants and smaller providers, however, those extra costs may be unbearable. Getting beyond the stalemate will require policy makers to focus on the goals the safe harbors were designed to achieve, including the growth and development of online platforms and services that produce and disseminate digital information. If we continue to believe, as Congress did when it enacted the DMCA,[82] that creating certainty for online businesses and their potential investors concerning the scope of copyright liability is an effective way to get and grow new platforms and services, then the design of the safe harbor regime should be optimized for certainty and for the encouragement of new entrants. Rights holders and Internet users, too, stand to benefit from greater certainty in the safe harbor regime; they, too, have borne the cost of ambiguity.

In the design of laws, optimizing for certainty will generally dictate a preference for rules over standards.[83] With rules, legislators give content to the

[79] Maria A. Pallante, *The Next Great Copyright Act*, 36 COLUM. J.L. & ARTS 315, 329 (2013).

[80] *See Register's Perspective on Copyright Review: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 30-32 (2015) (statement of Maria A. Pallante, Register of Copyrights and Director, U.S. Copyright Office) ("In the nearly twenty years since Congress enacted the DMCA, courts have stepped in to fill perceived gaps in the statutory framework, often interpreting provisions in ways that some believe run counter to the very balance that the DMCA sought to achieve.").

[81] *Id*.

[82] *See supra* notes 9-10 and accompanying text.

[83] *See* Duncan Kennedy, *Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1685, 1688 (1976) ("[T]he two great social virtues of formally realizable rules, as opposed to standards or principles, are the restraint of official arbitrariness and certainty."). This is not to say, of course, that standards are hopelessly unpredictable in their application. Over time, and with repeated adjudication, they can become more rule-like in their

law ex ante, before individuals act, whereas with standards, courts give content to the law ex post, after individuals act.[84] Rules provide clearer notice of the law because the content of rules is knowable and fairly certain as soon as they are promulgated.[85] Rules thus facilitate the design of compliant operating models for businesses.[86] Standards are more flexible and therefore somewhat less predictable than rules in their application.[87] This gives standards the virtue of promoting caution and discouraging opportunistic workarounds on the part of actors subject to them.[88] But standards can make business planning difficult because compliance can be assessed only ex post, through adjudication of particular cases.[89] Planning-related difficulties under a standards-based regime are further exacerbated if legal interpretations of the applicable standards conflict or if there is a dearth of precedent applying the standards to differing factual situations.[90] There is also a preference for rules over standards in scenarios involving a high frequency of regulated activity for similarly situated actors and actions.[91] In such scenarios, rules are more efficient than standards

predictability. *See, e.g.*, Matthew Sag, *Predicting Fair Use*, 73 OHIO ST. L.J. 47 (2012) (arguing, based on an empirical assessment of 280 cases, that fair use doctrine is more consistent than is usually assumed); Pamela Samuelson, *Unbundling Fair Uses*, 77 FORDHAM L. REV. 2537, 2541 (2009) (arguing that cases applying copyright's fair use standard fall into "common patterns" or "policy-relevant clusters").

[84] Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557, 559-60 (1992).

[85] *See id.* at 607-08 ("Thus, even when rules will be less accurate in providing results that are appropriate to actual circumstances—which they often will not be—they will tend to provide clearer notice than standards to individuals at the time they decide how to act." (footnote omitted)).

[86] *Cf. id.* at 585 (explaining that rules are available to individuals when they act and can therefore guide their action).

[87] *See id.* at 587 ("There may be inconsistency under a standard—as one might expect, for example, when decision is by general jury verdict. This could involve occasional aberrations or situations in which, say, a standard yielded one result half of the time and a different result the rest of the time." (footnotes omitted)).

[88] *Cf.* Joseph William Singer, *The Rule of Reason in Property Law*, 46 U.C. DAVIS L. REV. 1369, 1374 (2013) ("Standards promote useful moral reflection and deter socially destructive behavior. Fuzziness at the edges of rules often prompts better decision making, both by market actors and by judges.").

[89] *See* Kaplow, *supra* note 84, at 607-08 ("[I]ndividuals may not have effective notice of the result an adjudicator would reach [when applying a standard] and thus would be unable to act in light of it.").

[90] *See id.* at 612-13 (explaining that predictability in the application of standards may be costly and delayed because precedent, which gives standards their ex post content, develops slowly over the course of many adjudications, and cautious courts may delay that development by declining to make broad rulings that will cover future cases).

[91] *Id.* at 621 ("If conduct will be frequent, the additional costs of designing rules—which are borne once—are likely to be exceeded by the savings realized each time the rule is

because they can be applied across the board, whereas standards can be given content only on a case-by-case basis.[92]

Because a cooperative online enforcement regime delineating clear eligibility criteria for service providers was a primary policy goal of the DMCA safe harbors, and because the volume of activity to be regulated through the safe harbor framework is almost inconceivably high, Congress should have opted for rules over standards when designing the safe harbors. Instead, Congress created a hybrid design that mixes rules for notice in § 512(c)(3)(A) with a red flag standard in § 512(c)(1)(A). The hybrid design appears at first blush to offer the best of both worlds: the certainty that comes with the relative predictability of rules and the incentive to behave cautiously that comes with the relative unpredictability of standards. Experience has shown, however, that the actual costs of unpredictability in this arena have outweighed the potential benefits. By introducing an ambiguous notice standard into a regime otherwise defined by bright-line rules, Congress failed to align the design of the safe harbors with their primary purpose.[93] Moreover, by leaving the definition of red flag knowledge to courts, which rights holders have urged to interpret the provision expansively, Congress paved the way for disruption of the balance of enforcement burdens it specified in the notice-and-takedown protocol. In that balance, rights holders bear the costs associated with notice, including the cost of monitoring for infringements, and service providers bear the costs associated with content removal.[94]

As discussed above, courts so far have been unwilling to interpret the red flag provision to require investigation by service providers when they have

applied. . . . [W]hen behavior subject to the relevant law is frequent, standards tend to be more costly and result in behavior that conforms less well to underlying norms.").

[92] *See id*.

[93] John Blevins proposes that the key to managing the uncertainty of the red flag standard is having courts interpret it as a bright line rule. Blevins, *supra* note 34, at 1877-82. The conversion of the red flag standard into a rule through precedent would reduce the standard's inherent uncertainty. *See* Kaplow, *supra* note 84, at 577-79 (discussing how standards can become rules over time through successive adjudications). At the end of the day, however, many—if not most—questions concerning which facts and circumstances make infringing activity obvious to a reasonable person will end up being jury questions. Moreover, the expense of converting a standard into a rule through repeated adjudications can be substantial for entities to which the standard applies. *See id*. at 579 ("If acts will be frequent, there may be substantial costs in the interim under standards—costs of advice or costs reflected in behavior that does not comply with the law—that are avoided under rules."). Therefore, it may not be possible for judges to convert the red flag standard into a bright line rule through precedent—and even if it is possible, it may be expensive and time-consuming to an extent that chills innovation.

[94] *See* Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1113 (9th Cir. 2007) ("The DMCA notification procedures place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting infringement—squarely on the owners of the copyright.").

generalized knowledge of infringement on their systems. But even in the wake of decisions limiting the scope of red flag knowledge to facts and circumstances indicating specific instances of infringement, the content of the standard remains elusive and case-specific. The red flag standard creates a duty for service providers to investigate potential infringements in an unspecified range of circumstances knowable only ex post. That amorphous duty undermines the balance of burdens struck in the safe harbors, as well as the certainty of the safe harbors' scope. Given that the red flag standard implies *some* duty to investigate *some* subset of the universe of potential infringements on a provider's service, the DMCA's no-duty-to-monitor rule in § 512(m) can provide only a false sense of security for service providers. Some service providers defending suits alleging culpable inaction in the face of red flag knowledge have voluntarily implemented wholesale monitoring, a burden of which § 512(m) plainly relieves them.[95] Rights holders surely view this development as a benefit of the statute's mix of rules and standards, but it is hard to argue in light of § 512(m) that Congress intended proactive monitoring to be a soft condition for safe harbor protection.

Time and experience have shown that the red flag provision in the safe harbors makes their scope unworkably uncertain, raising operating and legal costs for potentially eligible service providers. The provision has also proven difficult for courts to reconcile with the express no-duty-to-monitor rule in § 512(m).[96] To better serve the policy goals of providing certainty and a clear division of enforcement burdens between rights holders and service providers, Congress should consider making actual knowledge the exclusive scienter standard for safe harbor disqualification in cases involving claims of contributory infringement against eligible service providers.[97] Such knowledge

[95] Among service providers that have asserted the DMCA safe harbors in litigation, YouTube, Veoh, MySpace, Myxer, Hotfile, and Vimeo voluntarily implemented digital fingerprinting systems for filtering user-uploaded content either before or during the pendency of the litigation. *Veoh II*, 667 F.3d 1022, 1028 (9th Cir. 2011), *withdrawn and superseded on reh'g*, 718 F.3d 1006 (9th Cir. 2013); Disney Enters., Inc. v. Hotfile Corp., No. 11-20427-CIV., 2013 WL 6336286, at *12 (S.D. Fla. Sept. 20, 2013); Capitol Records, LLC v. Vimeo, LLC, 972 F. Supp. 2d 500 (S.D.N.Y. 2013); Arista Records LLC v. Myxer Inc., No. CV 08-03935-GAF, 2011 WL 11660773, at *5 (C.D. Cal. Apr. 1, 2011); *YouTube I*, 718 F. Supp. 2d 514, 528 (S.D.N.Y. 2010), *aff'd in part, vacated in part*, 676 F.3d 19 (2d Cir. 2012); UMG Recordings, Inc. v. MySpace, Inc., 526 F. Supp. 2d 1046, 1054-55 (C.D. Cal. 2007); Darnell Witt, *Copyright Match on Vimeo*, VIMEO BLOG (May 21, 2014), https://vimeo.com/blog/post/copyright-match-on-vimeo [https://perma.cc/6A4B-JS5W].

[96] *See supra* note 39.

[97] This deviates from the common law standard for contributory infringement, which allows for both actual and constructive knowledge. *See generally* R. Anthony Reese, *The Relationship Between the ISP Safe Harbors and the Ordinary Rules of Copyright Liability*, 32 COLUM. J.L. & ARTS 427 (2009) (exploring the non-identical relationship between DMCA safe harbor standards and corresponding common law copyright liability standards). Courts deciding safe harbor cases involving vicarious infringement claims have held that

could be proven directly or circumstantially, through § 512(c) notifications or any other evidence showing the provider's subjective awareness of infringement acquired during operation of its service.

If tightening the scienter standard is politically infeasible, Congress could mitigate some bad effects of the red flag standard by eliminating or dramatically decreasing the exposure of service providers to statutory damages in cases involving allegations of red flag knowledge against providers that respond promptly to § 512(c) notifications.[98] Limiting statutory damages would lower the risk associated with litigating safe harbor eligibility to judgment and could, over time, lead to a wider range of adjudicated cases that give more stable (and rule-like) content to the red flag standard.

The notice-and-takedown framework at the heart of the safe harbors is rule-based by design. By planting the red flag standard in the middle of that design, Congress created a notice failure that it should fix in the current round of copyright reform. Service providers seeking safe harbor—and, for that matter, rights holders seeking to enforce their rights—should be able to know with certainty what actionable notice is (and what it is not).

II. NO NOTICE: DOMAIN NAME SEIZURES UNDER THE PRO-IP ACT

For all of the signaling problems that uncertain notice can cause, it is at least better than no notice at all. Lack of notice to domain name registrants prior to the seizure and civil forfeiture of Internet domain names under criminal copyright law is the second notice failure this article explores.[99] The notice

some alteration of common law standards is necessary to give the safe harbors their intended scope. *See YouTube II*, 676 F.3d 19, 37-38 (2d Cir. 2012) (holding that "'the right and ability to control' infringing activity under § 512(c)(1)(B) 'requires something more than the ability to remove or block access to materials posted on a service provider's website,'" even if the ability to remove or block access to infringing materials is sufficient on its own under the common law to establish the control element of a claim for vicarious infringement (quoting Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 645 (S.D.N.Y. 2011))).

[98] Wholesale reconsideration of the Copyright Act's statutory damages regime is necessary in any event. Many commentators have criticized the current regime for being excessive—potentially wildly so—in the recovery allowed for rights holders. *See, e.g.*, Peter S. Menell, *This American Copyright Life: Reflections on Re-Equilibrating Copyright for the Internet Age*, 61 J. COPYRIGHT SOC'Y U.S.A. 235, 317 (2014) (arguing that the potential availability of "astronomical statutory damages has undermined the balance sought in the DMCA's safe harbor regime"); Pamela Samuelson & Tara Wheatland, *Statutory Damages in Copyright Law: A Remedy in Need of Reform*, 51 WM. & MARY L. REV. 439, 443 (2009) (arguing that grossly excessive claims for statutory damages in cases involving allegations of secondary infringement against technology companies can have chilling effects on innovation, investment, and free speech).

[99] Substantial portions of this Part are adapted or reproduced from Annemarie Bridy, *Carpe Omnia: Civil Forfeiture in the War on Drugs and the War on Piracy*, 46 ARIZ. ST. L.J. 683 (2014). Citations in this Part are to the original source material cited in that article.

failure represented by ex parte domain name seizures sounds in two distinct areas of constitutional law—the Fifth Amendment's Takings Clause and the First Amendment's Free Speech Clause. Under a straightforward application of existing Supreme Court precedents in both areas, seizing domain names without prior notice to their registrants offends the Constitution. To achieve deterrent effects that are transitory at best in the online environment, the civil forfeiture of Internet domain names exacts disproportionately high constitutional costs and undermines the legitimacy and accountability of law enforcement.

A. *Copyright Crimes, Civil Forfeiture, and Domain Name Seizures*

The legal authority for domain name seizures comes from the PRO-IP Act of 2008, which gave the federal government power to seize and civilly forfeit property allegedly tainted by copyright crime.[100] Forfeiture, simply put, is an uncompensated taking of private property that the government alleges to be connected to criminal activity in some way.[101] The PRO-IP Act permits civil forfeiture of (1) criminally infringing articles, (2) direct or indirect proceeds of the production or distribution of infringing articles, and (3) property used or intended to be used to commit or facilitate the production or distribution of infringing articles.[102]

Since 2010, with the launch of Operation in Our Sites ("OIOS") by the Department of Homeland Security ("DHS"), the federal government has interpreted the PRO-IP Act to permit the ex parte seizure of Internet domain names in addition to the tangible forms of property that have traditionally been subject to civil forfeiture.[103] On the government's theory, domain names fall

---

[100] *See* Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008, Pub. L. No. 110-403, § 206, 122 Stat. 4256, 4262-63 (codified at 18 U.S.C. § 2323 (2012)) (amending criminal copyright law to, inter alia, add civil and criminal forfeiture as remedies).

[101] *See* JOHN L. WORRALL, U.S. DEP'T OF JUSTICE, OFFICE OF CMTY. ORIENTED POLICING SERVS., PROBLEM-ORIENTED GUIDES FOR POLICE: ASSET FORFEITURE 1 (2008).

[102] 18 U.S.C. § 2323(a)(1)(A)-(C).

[103] *See* U.S. INTELL. PROP. ENF'T COORDINATOR, EXEC. OFFICE OF THE PRESIDENT, 2013 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT 65 (2013).

The government's position that domain names are forfeitable under § 2323 is tenable with respect to websites that sell infringing or counterfeit hard goods. Such domain names pretty clearly facilitate the distribution of infringing articles. *See* 17 U.S.C. § 506 (2012); 18 U.S.C. § 2323. Query, however, whether the position can be defended with respect to domain names whose operators deliver infringing streams of copyrighted material, because streaming is not a distribution within the meaning of the Copyright Act. *See* Hearst Stations Inc. v. Aereo, Inc., 977 F. Supp. 2d 32, 40 (D. Mass. 2013) (clarifying that under the Copyright Act, streaming is a public performance rather than a distribution). Moreover, with respect to websites that actually do distribute digital files of copyrighted works via download, it is not clear that such files are "articles" for purposes of the PRO-IP Act. *Cf.* ClearCorrect Operating, LLC v. Int'l Trade Comm'n, No. 2014-1527, 2015 WL 6875205, at

into the third category of forfeitable property, commonly called facilitation property.[104] Of the three categories of forfeitable property, facilitation property has the weakest nexus to criminal activity.[105] Although such property can be used in connection with crime, it usually has a range of lawful uses. Consider, for example, a car whose trunk contains unauthorized DVDs of copyrighted movies, the DVD burner with which the unauthorized DVDs were made, or the warehouse in which the DVDs were temporarily stored. Because facilitation property often has an attenuated link to criminality and is generally dual-use in nature, its forfeiture warrants closer constitutional scrutiny than does the forfeiture of contraband, which is inherently illegal to possess.[106]

DHS agents initiated OIOS in 2010 by securing seizure warrants against ten domain names of websites offering first-run movies.[107] By 2012, OIOS was operating at full throttle. In February, "Operation Fake Sweep" saw the seizure of sixteen sites suspected of illegally streaming live sports telecasts and 291 sites suspected of selling counterfeit merchandise.[108] In July, "Project Copy Cat" closed down seventy additional sites suspected of selling counterfeit merchandise.[109] OIOS seizures continued through the fall of 2012 and into the winter holidays. In September and October, "Project Bitter Pill" targeted 686

*5 (Fed. Cir. Nov. 10, 2015) (holding that the word "articles" in the Tariff Act is limited to material things and does not include digital data).

[104] *See, e.g.*, Seizure Warrant, *In re* Seizure of Rapgodfathers.com, No. 10-2822M (C.D. Cal. Nov. 30, 2010) (averring that the domain names are forfeitable under 18 U.S.C. § 2323(a)(1)(B), which deals with facilitation property).

[105] *Cf.* David Pimentel, *Forfeitures Revisited: Bringing Principle to Practice in Federal Court*, 13 NEV. L.J. 1, 3 (2012) ("The policy justifications [for facilitating-property forfeitures] are by far the weakest, and the injustices and inequities—including the impact on innocent owners—are the most problematic in this category.").

[106] *See* Bennis v. Michigan, 516 U.S. 442, 460 (1996) (Stevens, J., dissenting) ("Forfeiture is more problematic for [facilitation] property than for [contraband or proceeds], both because of its potentially far broader sweep, and because the government's remedial interest in confiscation is less apparent.").

[107] U.S. Immigration & Customs Enf't, *"Operation In Our Sites" Targets Internet Movie Pirates ICE, Manhattan U.S. Attorney Seize Multiple Web Sites for Criminal Copyright Violations*, IBCAP (May 22, 2014), https://ibcap.us/operation-in-our-sites-targets-internet-movie-pirates-ice-manhattan-u-s-attorney-seize-multiple-web-sites-for-criminal-copyright-violations/ [https://perma.cc/A6D2-VQCU]. It is not clear from the press release whether the sites were offering program streams or downloads.

[108] *Agents and Officers Seize More than $4.8 Million in Fake NFL Merchandise and Seize 307 Websites During 'Operation Fake Sweep,'* U.S. IMMIGR. & CUSTOMS ENFORCEMENT (Feb. 2, 2012), https://www.ice.gov/news/releases/agents-and-officers-seize-more-48-million-fake-nfl-merchandise-and-seize-307-websites [https://perma.cc/36R4-AGUX].

[109] *ICE-Led IPR Center Seizes 70 Websites Duping Consumers into Buying Counterfeit Merchandise*, U.S. IMMIGR. & CUSTOMS ENFORCEMENT (July 12, 2012), https://www.ice.gov/news/releases/1207/120712washington.htm [https://perma.cc/83W6-LXFT] [hereinafter *ICE Seizes 70 Websites*].

sites suspected of selling counterfeit pharmaceuticals.[110] In November and December, "Project Cyber Monday" hit fifteen sites suspected of selling counterfeit sporting goods and eighty-nine sites suspected of selling other types of counterfeit goods.[111] In 2012 alone, DHS agents seized and administratively forfeited over 1,000 domain names on the theory that they were being used to facilitate criminal copyright infringement and trademark counterfeiting.[112] U.S.-based operators of the relevant domain name registries were ordered to redirect web traffic from the seized domains to a site displaying an anti-piracy banner featuring the logos of the Department of Justice ("DOJ") and DHS's Homeland Security Investigations.[113]

Outside the ambit of OIOS, the government executed its highest-profile ex parte seizure of domain names under criminal copyright law when it seized ten domain names associated with the New Zealand-based cyberlocker Megaupload in 2012.[114] The Megaupload seizures stand out from the vast majority of civil forfeitures, including those under OIOS, because they were accompanied by a criminal indictment of the site's operator, Kim Dotcom.[115] For reasons that will be explained below, it was much easier as a legal matter

[110] *HSI Seizes 686 Websites Selling Counterfeit Medicine to Unsuspecting Consumers*, U.S. IMMIGR. & CUSTOMS ENFORCEMENT (Oct. 3, 2012), https://www.ice.gov/news/releases/1210/121004washingtondc.htm [https://perma.cc/QWG4-ND75] ("In the largest operation of its kind, 100 countries took part in an international week of action targeting the online sale of counterfeit and illegal medicines.").

[111] *Houston HSI Seizes 89 Websites Selling Counterfeit Goods*, U.S. IMMIGR. & CUSTOMS ENFORCEMENT (Dec. 20, 2012), https://www.ice.gov/news/releases/1212/121220houston.htm [https://perma.cc/XHE3-3MF5]; *Upstate New York Man Arrested, 15 Websites Seized as Part of Global Crackdown on 'Cyber Monday,'* U.S. IMMIGR. & CUSTOMS ENFORCEMENT (Nov. 26, 2012), https://www.ice.gov/news/releases/upstate-new-york-man-arrested-15-websites-seized-part-global-crackdown-cyber-monday [https://perma.cc/MNT2-9XLG].

[112] *See supra* notes 108-11 and accompanying text.

[113] *See* Seizure Warrant, *supra* note 104 (requiring the domain name registry Verisign to redirect browser traffic from the Internet Protocol (IP) address of the seized domain name owner's server to an IP address belonging to an Immigration & Customs Enforcement server).

[114] The application for a seizure warrant in *United States v. Dotcom* asserted that the domain names were forfeitable under multiple provisions of the criminal code, including the PRO-IP Act, 18 U.S.C. § 2323 (2012) (civil forfeiture), and the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1963 (criminal forfeiture). *See* Application for a Warrant to Seize Property Subject to Forfeiture, *In re* Seizure of the Domain Name Megaupload.com and Nine Associated Domain Names, No. 1:12-sw-34 (E.D. Va. Jan. 13, 2012), ECF No. 145-1 (citing as authority 18 U.S.C. §§ 981(a)(1)(C), 982(a)(1), 1963(a), and 2323).

[115] *See* Indictment at 1, United States v. Dotcom, No. 1:12-cr-00003 (E.D. Va. Jan. 5, 2012), ECF No. 1 (bringing counts of, inter alia, conspiracy to commit copyright infringement, criminal copyright infringement, and aiding and abetting criminal copyright infringement).

for federal agents to seize and forfeit the Megaupload domain names than it has been for the DOJ to secure Kim Dotcom's extradition from New Zealand to the United States so that he can stand trial for his alleged copyright crimes.[116]

More recently, in September 2015, the FBI and the DOJ, acting on information from the RIAA, seized domain names associated with the file-sharing website ShareBeast.com.[117] The site was alleged to be responsible for unauthorized pre-release leaks of recordings by major-label rap artists, including Kanye West, Drake, Big Sean, and A$AP Rocky.[118] According to the RIAA, ShareBeast.com provided access to over 100,000 unauthorized music files for which the RIAA sent DMCA takedown notices.[119] In addition to seizing ShareBeast.com, the government seized the domain names of two related sites, albumjams.com and mp3pet.com.[120] The DOJ did not file any criminal charges against the operators of the sites at the time of the domain name seizures.

Before passage of the PRO-IP Act, property seizures were not entirely alien to copyright law. Under civil copyright law going back to the 1909 Act, plaintiffs have been able to get court orders for the impoundment and destruction of infringing goods and equipment used to manufacture them.[121] Civil forfeiture differs in important ways, however, from impoundment and destruction. Orders of impoundment and destruction may be issued by a court only in the context of a copyright infringement action.[122] Orders of

[116] *Cf.* Kim Zetter, *Judge Rules Kim Dotcom Can Be Extradited to US to Face Charges*, WIRED (Dec. 22, 2015, 5:50 PM), http://www.wired.com/2015/12/kim-dotcom-extradition-ruling/ [https://perma.cc/JU9C-YMLU] (reporting on a New Zealand court's ruling that Kim Dotcom can be extradited to the United States, four years after U.S. authorities filed criminal copyright charges against him).

[117] *See Department of Justice Takes Action Against Sharebeast*, RIAA (Sept. 13, 2015), https://www.riaa.com/department-of-justice-takes-action-against-sharebeast/ [https://perma.cc/NH8S-M82J]; *see also* Dave Calpito, *File-Sharing Site ShareBeast's Domain Seized by the FBI*, TECH TIMES (Sept. 15, 2015, 10:23 AM), http://www.techtimes.com/articles/84396/20150915/file-sharing-site-sharebeast-s-domain-seized-by-the-fbi.htm [https://perma.cc/U6AG-B7MJ].

[118] *See* Calpito, *supra* note 117.

[119] *Department of Justice Takes Action Against Sharebeast*, *supra* note 117.

[120] Calpito, *supra* note 117.

[121] *See* 17 U.S.C. § 503(a) (2012) (providing for impoundment and destruction of infringing copies and the means of reproducing them); Act of Mar. 4, 1909, ch. 320, § 25(c)-(d), 35 Stat. 1075, 1081 (providing for impoundment and destruction respectively); *see also* 4 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHTS § 14.07 (Rev. ed. 2013) (describing the parameters of impoundment and destruction under 17 U.S.C. § 503).

[122] *See* 17 U.S.C. § 503(a) (providing that the court may order impoundment on terms that it deems reasonable "[a]t any time while an action under this title is pending"); *id.*

impoundment can issue before a final judgment, but they must meet the strict standard for a preliminary injunction.[123] Orders of destruction can issue only upon final judgment.[124] By contrast, civil forfeiture of allegedly tainted property can occur regardless of whether the government brings a claim of criminal infringement against the property owner.[125] It can occur, for that matter, even if the government brings and fails to prove a claim of criminal infringement.[126] Moreover, arrest warrants for property subject to civil forfeiture are issued on a mere showing of probable cause.[127]

In cases involving civil forfeiture, the court's jurisdiction operates in rem, justified by the legal fiction that the property itself, and not the property owner, is legally culpable.[128] The in rem fiction allows courts, through property, to act on property owners like Kim Dotcom, who live abroad.[129] Although in rem jurisdiction still requires that the property owner have minimum contacts with

§ 503(b) (providing that the court may order destruction of impounded property "[a]s part of a final judgment or decree").

[123] *See* WPOW, Inc. v. MRLJ Enters., 584 F. Supp. 132, 135 (D.D.C. 1984); Paul S. Owens, *Impoundment Procedures Under the Copyright Act: The Constitutional Infirmities*, 14 HOFSTRA L. REV. 211, 226 (1985) (stating that the "clear trend" under the 1976 Act's impoundment provision is for a court to "order impoundment and issue a writ of seizure contemporaneously with the issuance of a temporary restraining order or a preliminary injunction," effectively conditioning the issuance of the writ on a Rule 65 showing of irreparable injury and a likelihood of success on the merits (footnote omitted)).

[124] 17 U.S.C. § 503(b).

[125] *See* Craig Gaumer, *A Prosecutor's Secret Weapon: Federal Civil Forfeiture Law*, U.S. ATTORNEYS' BULL., Nov. 2007, at 62 (pointing out that property may be subject to civil forfeiture even if the property owner is never charged, or is charged and ultimately acquitted).

[126] That is true because the government's burden of proof in a civil forfeiture case is preponderance of the evidence, whereas its burden in a criminal case is beyond a reasonable doubt. *See* Stefan D. Cassella, *Overview of Asset Forfeiture Law in the United States*, U.S. ATTORNEYS' BULL., Nov. 2007, at 17 (discussing the differing burdens of proof and citing the lack of a need for criminal conviction as a tactical advantage of civil forfeiture for prosecutors).

[127] Gaumer, *supra* note 125, at 71.

[128] *Contra* Cassella, *supra* note 126, at 15 ("At one time, it was said that civil forfeiture was based on the legal fiction that the property itself was guilty of the offense. That is no longer true. . . . The *in rem* structure of civil forfeiture is simply procedural convenience."). Civil forfeiture differs in this respect from criminal forfeiture, in which the court's jurisdiction operates in personam. *Id*. at 13-14. Property forfeited to the government through criminal forfeiture proceedings is forfeited as part of sentencing following the property owner's conviction. *Id*.; Worrall, *supra* note 101, at 3 (outlining the process of criminal forfeiture).

[129] *See* Shaffer v. Heitner, 433 U.S. 186, 206 (1977) ("[A]n adverse judgment *in rem* directly affects the property owner by divesting him of his rights in the property before the court.").

the forum, the property itself may provide the requisite contacts.[130] As long as the subject property is located within the geographic limits of the court's jurisdiction, the property owner can be anywhere in the world.[131] For purposes of establishing in rem jurisdiction over domain names, which have no physical presence, Congress provided in the Anticybersquatting Consumer Protection Act ("ACPA") that a domain name is "located" where the entity through which the domain name is registered has its primary place of business.[132] Under that rule of situs, which has since been applied beyond the trademark context,[133] the government can civilly forfeit domain names associated with so-called foreign infringing sites that are registered with U.S.-based registrars, but hosted and otherwise operated outside the United States.[134] In this way, the in rem fiction gives U.S. copyright law extraterritorial reach that it otherwise could not have.

Under federal law, there are two types of civil forfeiture—judicial and administrative. The government must forfeit real property judicially,[135] meaning that it must file a complaint for forfeiture and observe the procedural rules associated with the filing of a civil complaint, including notice to the owner of the defendant property.[136] By contrast, personal property valued at less than $500,000 and cash of any value may be forfeited administratively (i.e., ex parte) on a showing of probable cause that the property is subject to

[130] *See id*. at 207.

[131] *Cf. id*. ("The presence of property may also favor jurisdiction in cases . . . where the defendant's ownership of the property is conceded but the cause of action is otherwise related to rights and duties growing out of that ownership.").

[132] *See* 15 U.S.C. § 1125(d)(2)(A) (2012) (providing that an in rem cybersquatting action against a domain name may be filed "in the judicial district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located"); Caesars World, Inc. v. Casears-Palace.com, 112 F. Supp. 2d 502, 504 (E.D. Va. 2000) (discussing the ACPA and concluding that "[e]ven if a domain name is no more than data, Congress can make data property and assign its place of registration as its situs").

[133] *See* Office Depot Inc. v. Zuccarini, 596 F.3d 696, 702 (9th Cir. 2010) ("Although the current proceeding is not an action under the ACPA, the statute is authority for the proposition that domain names are personal property located wherever the registry or the registrar are located.").

[134] Many of the registrants whose domain names have been seized in OIOS are foreign nationals over whom U.S. courts likely have no in personam jurisdiction. *Cf. Operation in Our Sites Protects American Online Shoppers, Cracks Down on Counterfeiters*, U.S. IMMIGR. & CUSTOMS ENFORCEMENT (Nov. 27, 2011), https://www.ice.gov/news/releases/1111/111128washingtondc.htm [https://perma.cc/9D4L-82XL] (reporting that goods from seized websites were shipped from suppliers located abroad).

[135] *See* 18 U.S.C. § 985(a).

[136] *See* Cassella, *supra* note 126, at 16 ("The government, as plaintiff, files a verified complaint alleging that the property in question is subject to forfeiture pursuant to the applicable forfeiture statute, and claimants are required to file claims to the property and to answer the forfeiture complaint within a certain period of time.").

forfeiture under an applicable statute.[137] An arrest warrant is generally required for an administrative forfeiture.[138] Following the property's seizure, the owner or an interested third party may file a claim on it.[139] If that occurs, the government must convert the administrative forfeiture to a judicial one by filing a civil complaint for forfeiture in federal district court.[140] If the case reaches a court, the government's burden is to show by a preponderance of the evidence that the property is forfeitable.[141] If no claim is filed, however, the administratively seized property is summarily forfeited to the government without any adversary hearing or other judicial intervention.[142] The seizing agency simply files a declaration of forfeiture when the time for filing a claim lapses, and that declaration has the legal effect of a judgment.[143] In the vast majority of administrative forfeiture cases, the forfeitures are uncontested,[144] so the government is seldom put to its proof.

B. *Notice Failure and the Fifth Amendment*

It is a clearly established principle of procedural due process that parties whose property rights are to be affected in a legal proceeding are entitled to an opportunity to be heard and to prior notice so that they can exercise their right to be heard.[145] The constitutional prohibition on state takings of private property without due process of law "reflects the high value, embedded in our constitutional and political history, that we place on a person's right to enjoy

---

[137] *See id*. at 12-13; Gaumer, *supra* note 125, at 63 (describing procedures for administrative forfeitures).

[138] Cassella, *supra* note 126, at 13 (stating that seizure of the forfeited property "generally must be pursuant to a judicial warrant," but listing exceptions to the warrant requirement, including cases of seizure incident to lawful arrest and cases in which the property is mobile).

[139] *Id*. (explaining that the agency must give notice of its intent to forfeit the property "to anyone with a potential interest in contesting that action," and that anyone who contests the forfeiture must file a claim).

[140] *See id*. ("[I]f someone files a claim, the agency has [a] fixed period of time in which to refer the matter to a prosecutor for the commencement of a judicial forfeiture action, or to simply return the property."); Gaumer, *supra* note 125, at 63 ("[I]f a valid claim is filed with the agency . . . , the case must be referred to a USAO for commencement of a judicial forfeiture action, civil or criminal . . . .").

[141] *See* Cassella, *supra* note 126, at 15 ("In a civil forfeiture case, the government files a separate civil action *in rem* against the property itself, and then proves, by a preponderance of the evidence, that the property was derived from, or was used to commit, a crime.").

[142] *See id*. at 13 ("An administrative forfeiture is not really a proceeding, at all, in the judicial sense. It is more like an abandonment.").

[143] *Id*.

[144] *See id*. at 12 (stating that an estimated eighty percent of Drug Enforcement Agency forfeitures are uncontested and that "[o]ther seizing agencies report similar figures").

[145] Fuentes v. Shevin, 407 U.S. 67, 80 (1972).

what is his, free of governmental interference."[146] An exception to the requirement of prior notice and a hearing exists, but is reserved for "extraordinary situations where some valid governmental interest is at stake that justifies postponing the hearing until after the event."[147] In cases involving civil forfeitures, a narrowly defined exigent circumstances exception to the notice requirement applies if the property to be seized presents "a special need for very prompt action."[148] The classic exigent circumstances case involves property that can be moved to evade the court's in rem jurisdiction.[149] For property with which its owner cannot abscond, e.g., real property, the case law holds that pre-seizure notice is the rule unless some other exigent circumstance exists.[150]

The government gave no advance notice to registrants in the OIOS, Megaupload, and ShareBeast seizures, prompting the question of whether the exigent circumstances exception for movable property might excuse the notice requirement where the property to be forfeited is an Internet domain name. Although that is the assumption under which the government seems to be operating, the short answer is that domain name seizures do not fall under the movable property exception to civil forfeiture's notice requirement. The longer answer requires an explanation of the relationship between domain names and the digital content to which they provide access.

Online copyright enforcement is frequently described as a game of whack-a-mole or cat-and-mouse, because infringing content removed from one location frequently reappears seemingly instantaneously in another.[151] Infringement on

[146] *Id*. at 81.

[147] *Id*. at 82, 90-91 (quoting Boddie v. Connecticut, 401 U.S. 371, 378-79 (1971)).

[148] *Id*. at 91. Under *Fuentes*, the exigent circumstances test has three parts: (1) the seizure is directly necessary to secure an important governmental or general public interest; (2) there is a special need for very prompt action; and (3) the state has kept strict control over its monopoly of legitimate force, meaning that the person conducting the seizure is a government official responsible for determining its necessity. *Id*. at 90-91.

[149] *See, e.g*., Calero-Toledo v. Pearson Yacht Leasing Co., 416 U.S. 663, 679 (1974) (holding that lack of pre-seizure notice and hearing did not violate due process where the property seized was a yacht, which "could be removed to another jurisdiction, destroyed, or concealed, if advance warning of confiscation were given"); United States v. Any & All Radio Station Transmission Equip., 218 F.3d 543, 550 (6th Cir. 2000) (holding that "immediate seizure was necessary" because "the target of the government's forfeiture action was radio transmission equipment, which is movable personable property").

[150] United States v. James Daniel Good Real Prop., 510 U.S. 43, 62 (1993) ("Unless exigent circumstances are present, the Due Process Clause requires the Government to afford notice and a meaningful opportunity to be heard before seizing real property subject to civil forfeiture."); United States v. $129,727.00 U.S. Currency, 129 F.3d 486, 493 (9th Cir. 1997) (stating that the dispositive distinction for the Court in *James Daniel Good* was "the distinction between non-movable real property and movable personal property").

[151] *See, e.g*., Nate Anderson, *Rights Holders Tire of Takedown Whack-A-Mole, Seek Gov't Help*, ARSTECHNICA (May 4, 2010, 9:05 AM), http://arstechnica.com/tech-

the Internet is a moving target, but domain names are not; they stay put regardless of what happens to the content accessible through them. A technical explanation of what domain names are and how they work[152] makes it clear that they are not movable property, even though the content they make available can very easily be moved.

A domain name is a string of letters (e.g., Amazon.com) that corresponds to a string of numbers called an Internet Protocol ("IP") address (e.g., 205.251.242.54). Every piece of hardware connected to the Internet, including every server that acts as a website host, has a unique IP address.[153] IP addresses are hard to remember, but domain names are not. The Domain Name System ("DNS") was created to relieve people of the burden of having to keep track of long lists of IP addresses and the websites to which they correspond.[154] The DNS accomplishes this by means of a collection of databases called domain name registries. For each of the Internet's top-level domains (e.g., .com, .org, and .gov), there is a separate registry. Each registry is administered and controlled by a registry operator.[155] For every domain name in a given top-level domain, there is an entry in the registry that links the domain name to its corresponding IP address.[156] When a user enters the domain name of a website into the address bar of her web browser, the browser spontaneously routes a query to the appropriate registry to find the associated IP address and then retrieves content from that IP address, which is displayed to the user.[157] This process is called resolving a domain name.[158]

When the government seizes a domain name, it doesn't take physical custody of anything. Rather, it presents the relevant registry operator with a court order directing the operator to alter the database entry for that domain name so that it no longer resolves to the IP address designated by the

policy/2010/05/rightsholders-tire-of-takedown-whac-a-mole-seek-govt-help/ [https://perma.cc/G8DC-3YSR] ("In [content owners'] view, the law put too much onus on rightsholders to do the hard work of identifying files and sending out takedown notices—only to see some other 14-year old post the exact same *Simpsons* clip 20 minutes later.").

[152] *See* Office Depot Inc. v. Zuccarini, 596 F.3d 696, 698-99 (9th Cir. 2010).

[153] *See id*. at 698.

[154] *See* Marshall Brain & Stephanie Crawford, *How Domain Name Servers Work*, HOWSTUFFWORKS: TECH (April 1, 2000), http://computer.howstuffworks.com/dns.htm [https://perma.cc/E4CK-QZYQ].

[155] *See About gTLDs*, ICANN, https://www.icann.org/resources/pages/about-e5-2012-02-25-en [https://perma.cc/CC55-MT5D].

[156] *Office Depot*, 596 F.3d at 698.

[157] Brain & Crawford, *supra* note 154 ("[Y]our computer uses a DNS server to look up the domain name you're trying to access. . . . For example, when you enter [a domain name] in your browser, part of the network connection includes resolving the domain name . . . into an IP address . . . .").

[158] *Id*.

owner/registrant.[159] The seized domain name is made to resolve instead to a government-controlled IP address.[160] When the database entry is altered, nothing actually happens to the underlying website's content. The content remains under the control of the original owner/registrant and is still accessible on the open Web to anyone who actually knows the IP address—which no one, as a practical matter, does.[161] For this reason, it is misleading to speak, as ICE representatives often do, of "seizing a website."[162]

The structure of the DNS is such that the registry operator, which is wholly independent of individual domain name registrants, fully controls the registry and all of its constituent database entries.[163] A registrant can change the IP address to which her domain name corresponds and can cancel or decline to renew the registration, but she has no direct control over any entry in the registry and no ability to delete a domain name from it.[164] A registrant's dominion over a domain name is thus completely mediated by an independent registry operator.[165] To understand this point is to understand that seizing a domain name does not inherently present "a special need for very prompt action," as the Supreme Court's civil forfeiture precedents require for an exception to the notice rule.[166]

A domain name registrant can move the content associated with a domain name, but seizing the domain name will do nothing to prevent that because the content displayed on a website is physically separate from the domain name, which is really just a directional tool. Moreover, seizing a domain name in one

[159] *See supra* note 113 and accompanying text; *cf.* Palacio Del Mar Homeowners Ass'n, Inc. v. McMahon, 95 Cal. Rptr. 3d 445, 449 (2009) ("Domain name registration supplies the intangible 'contractual right to use a unique domain name for a specified period of time.' Even if this right constitutes property, it cannot be taken 'into custody.'" (first quoting Network Sols., Inc. v. Umbro Int'l, Inc., 529 S.E.2d 80, 86 (2000); and then quoting CAL. CIV. PROC. CODE § 699.040 (West 2016))).

[160] *See supra* note 113 and accompanying text.

[161] The fact that the content technically remains accessible following the seizure could be cited to support the argument that ex parte domain name seizures are not a prior restraint on speech. *See infra* Section II.C. There is an important distinction to be made, however, between speech that is accessible in theory and speech that is accessible in practice. Given the way the DNS works, breaking the link between a domain name and its corresponding IP address effectively takes the underlying content out of circulation, at least temporarily.

[162] *See, e.g.*, *ICE Seizes 70 Websites*, *supra* note 109.

[163] *See About gTLDs*, *supra* note 155.

[164] *See Cancel My Domain*, GODADDY, https://www.godaddy.com/help/cancel-my-domain-412 [https://perma.cc/7573-7XM5] ("You can cancel a domain name so that it is no longer registered to you. Depending on the type of domain name you cancel, the registry might hold it before releasing it for another user to register.").

[165] *See* Office Depot Inc. v. Zuccarini, 596 F.3d 696, 699 (9th Cir. 2010) ("Registrants interact with the registrars, who in turn interact with the registries.").

[166] Calero-Toledo v. Pearson Yacht Leasing Co., 416 U.S. 663, 678 (1974) (quoting Fuentes v. Shevin, 407 U.S. 67, 91 (1972)).

top-level domain will not prevent someone from registering the same domain name in another top-level domain or from associating the allegedly infringing content with a different domain name in the same top-level domain. Far from solving the whack-a-mole problem, seizing domain names simply perpetuates it.

Unlike a pirated DVD or a fake designer bag, domain names have no corporeal presence. The law treats them as personal property, but they're not movable like chattels, and that impacts what process is due when the government civilly forfeits them.[167] Unlike a yacht used to transport drugs or transmission equipment used to deliver pirate radio broadcasts—both of which courts have held *can* be seized without notice[168]—a domain name that provides access to infringing content cannot be moved to conceal it from government agents or to defeat the jurisdiction of a federal court. This distinction compels the conclusion that there is no self-evident exigency that justifies ex parte seizures of domain names.

Ex parte domain name seizures present amplified due process problems because they can have massive secondary effects, as when a seized domain name belongs to a public cyberlocker service that hosts the digital property of millions or tens of millions of users from all over the world. Users of Megaupload who attempted to access the site after its domain names were seized found a DOJ seizure banner in place of Megaupload's home page.[169] The banner was silent concerning whether or how users could claim their files. The files—totaling twenty-five million gigabytes on over 1,100 hard drives—

[167] *See* United States v. James Daniel Good Real Prop., 510 U.S. 43, 52 (1993) (explaining that the movability of the property in *Calero-Toledo* was an exigency that justified a due process exception). For a thorough discussion of the propertization of domain names and its legal consequences, see Anupam Chander, *The New, New Property*, 81 TEX. L. REV. 715, 776-79 (2003) and Greg Lastowka, *Decoding Cyberproperty*, 40 IND. L. REV. 23, 49-53 (2007). Scholars are split on whether treating domain names as property is good public policy. *Compare, e.g.*, Margaret Jane Radin, *Incomplete Commodification in the Computerized World*, *in* THE COMMODIFICATION OF INFORMATION 3, 7 (Niva Elkin-Koren & Neil Weinstock Netanel eds., 2002) (arguing that the propertization of information in cyberspace is dystopic), *with* Eli Noam, *Two Cheers for the Commodification of Information*, *in* THE COMMODIFICATION OF INFORMATION, *supra*, at 43 (arguing that propertization in cyberspace is beneficial because it aids in the creation, flow, and distribution of information).

[168] *Calero-Toledo*, 416 U.S. at 679; United States v. Any & All Radio Station Transmission Equip., 218 F.3d 543, 550 (6th Cir. 2000).

[169] *See* Lena Mualla, *With Its Recent Megaupload Indictment, the Government Gets Aggressive in Its Efforts to Curtail Copyright Infringement*, WAKE FOREST U.: J. BUS. & INTELL. PROP. L. (Apr. 7, 2012), http://ipjournal.law.wfu.edu/2012/04/with-its-recent-megaupload-indictment-the-government-gets-aggressive-in-its-efforts-to-curtail-copyright-infringement/ [https://perma.cc/DR5S-KQLR] (reproducing a copy of the seizure banner).

were stranded on servers belonging to Megaupload's hosting service, Virginia-based Carpathia Hosting.[170]

Legitimate users among the site's sixty million were left without recourse following the seizure.[171] Even if as many as ninety-five percent of Megaupload's users were inveterate infringers, the seizure left the digital property of at least three million non-infringers in legal limbo. Among them was an Ohio man named Kyle Goodwin, whose business, OhioSportsNet, makes and distributes videos of local high school sporting events.[172] Goodwin filed a motion with the court to claim his data.[173] Government lawyers opposed the motion, asserting that five separate factors had to be considered before the court could determine whether to order the data returned: (1) whether Goodwin had clean hands; (2) the cost and technical feasibility of finding a single user's data; (3) the number of other similarly situated parties; (4) how, if at all, the government could prevent returning infringing data along with non-infringing data; and (5) whether other, cheaper remedies existed for Goodwin.[174]

Although Goodwin stood accused of no crime, the government's seizure of the Megaupload domain names effectively deprived him of his property rights in the videos he lawfully stored with Megaupload on Carpathia's servers.[175] The burden was on him to retain counsel and figure out how to get his data back.[176] When Goodwin filed a motion for the return of his property, asking the court to exercise its equitable jurisdiction, the government asked the court to weigh in its favor the hassle of finding Goodwin's property among the petabytes of data stranded by the seizures.[177] It argued further that it should

[170] *See* David Kravets, *Feds Say No Dice in Retrieving Your Data Seized in Megaupload Case*, WIRED (Oct. 31, 2012, 5:17 PM), http://www.wired.com/threatlevel/2012/10/no-dice-megaupload-data/ [https://perma.cc/V97Y-Z8CN].

[171] *See id*. ("Federal prosecutors are proposing a process that would make it essentially impossible for former Megaupload users to recover their data following the government's seizure of the file-sharing service's servers and domain names . . . .").

[172] *See* Brief of Kyle Goodwin in Support of His Motion for the Return of Property Pursuant to 18 U.S.C. § 1963 and/or Federal Rule of Criminal Procedure 41(g) at 4-6, United States v. Dotcom, No. 1:12-cr-00003-LO (E.D. Va. May 25, 2012), ECF No. 91.

[173] *See* Motion of Kyle Goodwin for the Return of Property Pursuant to 18 U.S.C. § 1963 and/or Federal Rule of Criminal Procedure 41(g), United States v. Dotcom, No. 1:12-cr-00003-LO (E.D. Va. May 25, 2012), ECF No. 90.

[174] *See* Kravets, *supra* note 170 (quoting from the government's brief in opposition to Goodwin's motion).

[175] The Megaupload data were in legal limbo when Goodwin sought recovery of his files. *See id*. When Megaupload's assets were frozen, Carpathia stopped being paid for its hosting services. *See id*. ("Carpathia has said it is spending $9,000 daily to retain the data, and is demanding that Judge O'Grady relieve it of that burden.").

[176] *See id*. (explaining that there was "no clear process on how to return data to their rightful owners").

[177] *See* Response of the United States to Non-Party Kyle Goodwin's Motion for the Return of Property Pursuant to 18 U.S.C. § 1963 or Federal Rule of Criminal Procedure

have no obligation to locate Goodwin's property because it didn't seize the actual servers on which Goodwin's data were stored.[178] Goodwin's files got caught in the digital drift net of the Megaupload forfeiture, and the government had no interest in disentangling them.

Domain names can be a gateway to infringing content and a means of unlawful distribution for copyright criminals. The very same domain names, at the very same time, can provide access to cloud-based storage for millions of legitimate users like Kyle Goodwin. When dual-use property in which many parties have an interest is seized, the innocent are punished along with accused criminals. Goodwin's ability to access his property depended completely on Megaupload's property rights in its domain names, yet Goodwin got no advance notice that those domain names were subject to seizure.[179] Even if he had gotten advance notice, however, forfeiture law would not have helped him. The law does provide an innocent owner defense, which can be raised post-seizure, but that defense is available only to third parties who can prove they have an actual ownership interest in the seized property.[180] Goodwin owned property accessible through the seized domain names, but he had no property interest in the domain names themselves, so he lacked standing to raise an innocent owner defense.[181] In the government's view, Goodwin was merely "collaterally aggrieved" by the forfeiture, so it owed no duty to help him recover his property.[182]

41(g) at 3, United States v. Dotcom, No. 1:12-cr-00003-LO (E.D. Va. June 8, 2012), ECF No. 99 [hereinafter Response of the United States] ("The issue is that the process of identifying, copying, and returning Mr. Goodwin's data will be inordinately expensive.").

[178] *Id*. at 4.

[179] *See id*. at 10 ("Mr. Goodwin cites no law for the proposition that the government violates the Constitution by failing to notify a third party prior to the execution of a search or seizure warrant."); *see also* Cassella, *supra* note 126, at 13 ("Once the property has been seized, the agency commences the administrative forfeiture proceeding by sending notice of its intent to forfeit the property, to anyone with a potential interest in contesting that action and by publishing a notice in the newspaper.").

[180] Under federal civil forfeiture law, an innocent owner is defined as "a person with an ownership interest in *the specific property sought to be forfeited*." 18 U.S.C. § 983(d)(6)(A) (2012) (emphasis added). Similarly, under RICO, a third-party may petition for the return of forfeited property, but she must prove that she has "a legal right, title, or interest in *the property*." *Id*. § 1963(*l*)(6)(A) (emphasis added). When Goodwin moved to recover his property under RICO, the government argued that he had no standing because he had no cognizable interest in the forfeited property, i.e., Megaupload's domain names. *See* Response of the United States, *supra* note 177, at 5.

[181] *See* Response of the United States, *supra* note 177, at 5 ("Mr. Goodwin has asserted an interest in property that is neither restrained, nor seized, nor subject to forfeiture."); *see also* United States v. 74.05 Acres of Land, 428 F. Supp. 2d 57, 65 (D. Conn. 2006) ("[T]his court concludes that an equitable interest in property is not a sufficient ownership interest to grant a claimant statutory standing as an innocent owner.").

[182] Response of the United States, *supra* note 177, at 11.

When the government seized the Megaupload domain names, Kyle Goodwin and similarly situated Megaupload users experienced a secondary or derivative notice failure that denied them due process for what amounted to a governmental taking of their property. Because of the limited scope of the innocent owner defense under federal civil forfeiture law, Megaupload's non-infringing users suffered, in equity's parlance, a wrong without a remedy.[183] The government was not troubled to see the baby go down the drain with the bathwater—a nonchalance on the part of government agents that the framers intended the Fifth Amendment to check.

C. *Notice Failure and the First Amendment*

Domain names are not just gateways to vast repositories of digital property, they are also instrumentalities of speech.[184] Their seizure raises First Amendment concerns because a single domain name allegedly tainted by criminally infringing content may provide access to a mix of infringing and non-infringing speech. While infringing speech falls outside the scope of the First Amendment,[185] most non-infringing speech is constitutionally protected. Telling the difference between the two can be challenging for judges, even after the benefit of full discovery. When a domain name is seized, access to all of the speech displayed at or accessible through that domain is blocked without First Amendment scrutiny and without any proof beyond probable cause that any of the blocked speech is actually criminally infringing.[186] Once the domain name is in the government's "custody," the site's former operators are barred from further dissemination of speech at that domain, a restriction that implicates the First Amendment's prior restraint doctrine.[187] Although a site operator can associate the underlying content with a new domain name, the seized domain name no longer functions as an instrumentality of speech for the site's operator or its users. The seizure transforms the domain name into an instrumentality of speech for the government.

---

[183] *See, e.g.*, Indep. Wireless Tel. Co. v. Radio Corp. of Am., 269 U.S. 459, 472 (1926).

[184] *Cf.* Reno v. ACLU, 521 U.S. 844, 870 (1997) ("Our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to [the Internet].").

[185] *See, e.g.*, Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562, 574-75 (1977) (holding that the First Amendment does not immunize acts of copyright infringement); Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211, 220 (S.D.N.Y. 2000) ("[T]he Supreme Court . . . has made it unmistakably clear that the First Amendment does not shield copyright infringement.").

[186] *See* Seizure Warrant, *supra* note 104 (explaining the effect of a domain name seizure); *see also supra* notes 159-62 and accompanying text (describing how a domain name is seized).

[187] *See* Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 656 (E.D. Pa. 2004) (explaining that restrictions that "do not prevent speech from reaching the market place but remove material already available on the Internet from circulation" fall under the category of administrative prior restraints).

Paul Owens has argued with respect to the Copyright Act's impoundment procedures that the most rigorous constitutional safeguards should apply to pre-trial seizures of property that embodies First Amendment values, especially when that property is not itself allegedly infringing.[188] His position is supported by the Supreme Court's jurisprudence on seizures of property allegedly implicated in the production and distribution of obscene adult books and films.[189] In *Fort Wayne Books v. Indiana*, a state trial court issued an ex parte seizure order under Indiana's racketeering/civil forfeiture statute directing police to immediately seize all of the real estate, inventory, and other forfeitable personal property belonging to the plaintiff bookstore owner.[190] County sheriffs promptly padlocked the bookstore's three locations, and a few days later packed up and hauled off the stores' complete inventory.[191] No trial date on the civil forfeiture complaint was ever set.[192] The Indiana appellate court held that the seizure violated the First Amendment, but the Indiana Supreme Court disagreed.[193]

The United States Supreme Court granted cert and reversed the Indiana Supreme Court.[194] Citing its earlier decision in *Heller v. New York*,[195] the Supreme Court held that a showing of probable cause is constitutionally insufficient when First Amendment property is the target of civil forfeiture and the government's goal in seizing the property is to remove it from circulation.[196] Without an adversary hearing prior to the seizure, the Court said,

---

[188] Owens, *supra* note 123, at 247-48. Whereas a domain name can be *trademark* infringing, it cannot be *copyright* infringing. *See* 37 C.F.R. § 202.1(a) (2015) (excluding from copyright protection "[w]ords and short phrases such as names, titles, and slogans"); Moody v. Morris, 608 F. Supp. 2d 575, 579 (S.D.N.Y. 2009) ("[I]t is axiomatic that words, short phrases, titles, and slogans are not subject to copyright, even if they can be trademarked.").

[189] *See* Alexander v. United States, 509 U.S. 544 (1993) (involving federal RICO criminal forfeiture of real property and other assets of the petitioner's "hard core" adult entertainment businesses, and analyzing whether RICO's forfeiture provisions are constitutionally overbroad); Fort Wayne Books, Inc. v. Indiana, 489 U.S. 46 (1989) (involving state RICO civil forfeiture and a pre-trial seizure of petitioner's adult bookstore and all of its contents, and stating that the Court "has repeatedly held that rigorous procedural safeguards must be employed before expressive materials can be seized as 'obscene'").

[190] 489 U.S. at 51-52.

[191] *Id*. at 52.

[192] *Id*.

[193] *Id*. at 52-53.

[194] *Id*. at 62 ("We reverse, however, the judgment . . . sustaining the pretrial seizure order.").

[195] 413 U.S. 483 (1973).

[196] *See Fort Wayne Books*, 489 U.S. at 63 ("While a single copy of a book or film may be seized and retained for evidentiary purposes based on a finding of probable cause, the

the risk of prior restraint is too great.[197] By contrast, as the Court later held in *Alexander v. United States*, the risk of prior restraint is not present in cases involving criminal forfeiture because a criminal trial on the merits of the underlying offense affords adequate procedural safeguards to avoid premature forfeiture of protected expressive property.[198] These rulings strongly suggest that OIOS domain name seizures, which occur ex parte and which are intended to cut off access to expressive content, do not provide adequate protections to withstand First Amendment scrutiny.

ICE officials responded to the First Amendment critique of domain name seizures by assuring policy makers and the public that OIOS was "not targeting lawful businesses, blogs, or discussion boards" and that the targeted domain names were "commercial and . . . engaged in repeated and significant violation[s] of the law."[199] The truth, however, was more nuanced than that. Most of the domain names seized in the early phases of OIOS *were* gateways to online storefronts dedicated to the sale of blatantly counterfeit hard goods.[200] Domain names incorporating trademarked brand names—for example, cheap-louisvuitton-replica.com and buyviagrabrand.com—more or less self-identify as instrumentalities of infringement for commercial gain. Some of the domain names first targeted in OIOS, however, were gateways to a wider and more diverse collection of content. Dajaz1.com, which was seized in November 2010, and Rojadirecta.com and .org, which were seized in January 2011, are well-documented examples.[201]

publication may not be taken out of circulation completely until there has been a determination of obscenity after an adversary hearing.").

[197] *Id*. at 63-64.

[198] 509 U.S. 544, 552-53 (1993) (distinguishing *Fort Wayne Books* on the basis that "[h]ere . . . , the seizure was not premature, because the Government established beyond a reasonable doubt the basis for the forfeiture").

[199] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites: Hearing Before the Subcomm. on Intell. Prop., Competition, and the Internet of the H. Comm. on the Judiciary*, 112th Cong. 164 (2011) (statement of John Morton, Director, U.S. Immigration & Customs Enf't).

[200] *See* U.S. IMMIGRATION & CUSTOMS ENF'T, FACT SHEET: WEBSITES SEIZED DURING THE EIGHTH PHASE OF OPERATION IN OUR SITES (2011), https://www.ice.gov/doclib/news/releases/2011/111128washingtondc.pdf [https://perma.cc/2KCK-FAED] (listing 150 seized domain names).

[201] *See* Ben Sisario, *Hip-Hop Copyright Case Had Little Explanation*, N.Y. TIMES (May 6, 2012), http://www.nytimes.com/2012/05/07/business/media/hip-hop-site-dajaz1s-copyright-case-ends-in-confusion.html?_r=0 [https://perma.cc/6A5W-9BRD] (reporting on the Dajaz1 seizure); *New York Investigators Seize 10 Websites that Illegally Streamed Copyrighted Sporting and Pay-Per-View Events*, U.S. IMMIGR. & CUSTOMS ENFORCEMENT (Feb. 2, 2011), https://www.ice.gov/news/releases/new-york-investigators-seize-10-websites-illegally-streamed-copyrighted-sporting-and [https://perma.cc/69US-UENJ] (reporting on the Rojadirecta seizures).

Dajaz1 provided news and commentary on hip-hop culture along with links to pre-release music files that could be streamed or downloaded.[202] Rojadirecta indexed links to live streams of sporting events and hosted discussion forums for sports fans.[203] Both Dajaz1 and Rojadirecta were seized for facilitating criminal copyright infringement by linking to sites that illegally displayed, performed, or distributed copyrighted works.[204] The government did not allege that either site sold any infringing goods.[205] According to the government's own affidavit, Dajaz1 had not even earned revenue from displaying advertisements.[206] To label these sites "commercial" and their operators obvious IP criminals was at best a stretch.

In both cases, the sites' operators filed claims for return of the seized domain names, and in both cases, the government relented before its evidence could be tested against a standard more stringent than probable cause.[207] In the Dajaz1 case, no complaint for civil forfeiture was ever filed, despite the court's giving the government three extensions of time to file, adding up to a six-month delay.[208] In the Rojadirecta case, the government voluntarily dismissed

[202] *See* David Kravets, *Senator Wants Answers from DHS over Domain Name Seizures*, WIRED (Dec. 9, 2011, 7:34 PM), http://www.wired.com/threatlevel/2011/12/wyden-domain-seizure/ [https://perma.cc/HZX8-ZP98] (reporting on the Dajaz1 seizure and noting that some of the music posted on the site had been given to the site by the artists and labels).

[203] *See* Ryan Singel, *Oops! Copyright Cops Return Seized RojaDirecta Domain Names—19 Months Later*, WIRED (Aug. 29, 2012, 4:07 PM), http://www.wired.com/threatlevel/2012/08/domain-names-returned [https://perma.cc/A27R-8YZB].

[204] *See* Complaint at 8, United States v. Rojadirecta.org, No. 1:11-cv-04139-PAC (S.D.N.Y. June 17, 2011) (alleging that the Rojadirecta website "provided links to daily live sporting events and Pay-Per-View events, as well as downloadable sporting events or Pay-Per-View events that had previously been aired"); Application and Affidavit for Seizure Warrant at 53, *In re* Seizure of Rapgodfathers.com, No. 10-2822M (C.D. Cal. Nov. 30, 2010) [hereinafter Application for Seizure Warrant] (describing how the Dajaz1.com homepage "displays album covers and recording artist photographs, short descriptions, and links for numerous pirated songs").

[205] *See* Complaint, *supra* note 204, at 2-15 (claiming only that the Rojadirecta website was a "linking" website); Application for Seizure Warrant, *supra* note 204, at 53-58 (same).

[206] *See* Application for Seizure Warrant, *supra* note 204, at 57-58.

[207] The owner of the Rojadirecta domain names, Puerto 80 Projects, raised the First Amendment issue in a petition for release of property under 18 U.S.C. § 983(f) (2012). *See* Order Denying Petition at 3, Puerto 80 Projects v. United States, No. 1:11-cv-03983-PAC (S.D.N.Y. Aug. 4, 2011), ECF No. 15 (explaining Puerto 80's argument that seizure of the domain names "infringes on . . . users' and readers' First Amendment rights"). Without addressing the merits of the First Amendment argument, the court held that "the First Amendment considerations [raised by Puerto 80] certainly do not establish the kind of substantial hardship required to prevail on this petition." *Id*. at 4.

[208] *See* Order Extending for an Additional Sixty Days the Deadline for Filing of Civil Forfeiture Complaint, *Dajaz1.com*, No. 2:11-cm-00110-UA (C.D. Cal. Sept. 19, 2011), ECF No. 9; Order Extending for an Additional Sixty Days the Deadline for Filing of Civil Forfeiture Complaint, *Dajaz1.com*, No. 2:11-cm-00110-UA (C.D. Cal. July 18, 2011), ECF

its civil forfeiture complaint over a year and a half after gaining control of the two domain names.[209] In its request to vacate the Rojadirecta seizure warrant, the government referred elliptically to "certain recent judicial authority" germane to the case.[210] Given the timing of the request, that unnamed authority was most likely *Flava Works, Inc. v. Gunter*,[211] a Seventh Circuit decision that found no civil copyright infringement on the part of a social-bookmarking site, which embedded video that could be streamed by the site's users from another site's server.[212]

As the government correctly asserted in defense of OIOS,[213] speech accessible at an obviously trademark-infringing domain name that proposes the sale of blatantly counterfeit hard goods does not present a close case for First Amendment analysis. Such obviously unprotected speech, however, was not the kind of speech accessible at either Rojadirecta or Dajaz1. By the government's own tacit admission, the operators of those sites, upon closer consideration, were not blatant lawbreakers.

Proving the argument that the seizure process is prone to costly errors, the government has since retreated from other seizures it undertook in the early phases of OIOS.[214] OnSmash.com and Torrent-Finder.com, which were seized at the same time as Dajaz1, were unceremoniously transferred back to their operators in the fall of 2015, five years after their seizure.[215] When asked to explain why the government had declined to move forward with the cases, an ICE spokesman admitted that "there was not enough evidence to seize the websites."[216] From a business perspective, OnSmash never fully recovered,[217] but the government will pay no price for its misstep. Adding insult to injury,

No. 6; Order Extending for an Additional Sixty Days the Deadline for Filing of Civil Forfeiture Complaint, *Dajaz1.com*, No. 2:11-cm-00110-UA (C.D. Cal. May 13, 2011), ECF No. 3. All filings in the case were sealed until April 2012. *See* Order Unsealing Court Records, *Dajaz1.com*, No. 2:11-cm-00110-UA (C.D. Cal. Apr. 5, 2012), ECF No. 11.

[209] *See* Notice of Voluntary Dismissal, *Rojadirecta.org*, No. 1:11-cv-04139-PAC (S.D.N.Y. Aug. 29, 2012), ECF No. 55.

[210] Letter from Christopher D. Frey, Assistant U.S. Attorney, to Judge Paul A. Crotty, *Rojadirecta.org*, No. 1:11-cv-04139-PAC (S.D.N.Y. Aug. 29, 2012), ECF No. 56.

[211] 689 F.3d 754 (7th Cir. 2012).

[212] *Id.* at 756, 760 (vacating the district court's grant of a preliminary injunction against the bookmarking site).

[213] *See supra* note 199 and accompanying text.

[214] *See* Ben Sisario, *5 Years and $7 Later, U.S. Returns a Seized Hip-Hop Blog Site*, N.Y. TIMES, Jan. 2, 2016, at B1 (reporting on the return of OnSmash.com and Torrent-Finder.com).

[215] *Id.*; *see also* Ben Sisario, *Music Web Sites Dispute Legality of Their Closing*, N.Y. TIMES, Dec. 20, 2010, at B6 (reporting on the seizures and the protests of the affected website operators).

[216] Sisario, *supra* note 214.

[217] *See id.* (stating that OnSmash "has lost most of its momentum").

the government actually collected seven dollars—the appraised value of the domain name—from the site's operator.[218]

The danger in allowing ex parte seizure of domain names is that appropriate scrutiny of the government's actions generally never occurs. Lack of an adversary process gives ambitious law enforcement agents license to play fast and loose with the First Amendment when it comes to online copyright enforcement. Sites like Rojadirecta and Dajaz1 are tarred with the same brush as sites like cheap-louisvuitton-replica.com, even though they are very different kinds of sites. In the brick-and-mortar world, *Fort Wayne Books* prevents that from happening.[219] The same should be true in cyberspace, because seizing a domain name for alleged facilitation of copyright crime is the twenty-first-century equivalent of padlocking a bookstore.

D. *Fixing the Failure: Aligning Domain Name Seizures with Constitutional Minima*

Under Supreme Court precedents governing procedural due process in civil forfeiture cases, the Fifth Amendment requires pre-seizure notice and an opportunity to be heard in all cases unless there is "a special need for very prompt action," as where the property to be seized is movable.[220] Infringing content on the Internet is movable, but domain names are not.[221] With domain names, therefore, there is generally time for adversary process. In this respect, domain names are more like real property than they are like portable property for legal purposes. They should be treated as such procedurally when the government seeks to forfeit them.

The First Amendment imposes the same requirement of prior notice when government agents seek to forfeit expressive property with the aim of removing that property from circulation.[222] In such cases, an adversary hearing is required to mitigate the risk of prior restraint.[223] A statute purporting to regulate illegal speech offends the First Amendment when it provides that "a judge is only required to make a finding of probable cause, he can make this determination ex parte, and there is no requirement that the publisher or distributor receive notice or an opportunity to be heard."[224] Reflecting the extraordinarily high value our laws place on free expression, a showing of

---

[218] *Id*. ("Suing for the return of OnSmash would have been expensive and risky, so Mr. Hoffman pursued an 'offer in compromise' with the government—submitting a petition for the site's return, and paying what the government determined to be its appraised value: $7.").

[219] *See supra* notes 190-98 and accompanying text.

[220] *See, e.g*., Calero-Toledo v. Pearson Yacht Leasing Co., 416 U.S. 663, 678-79 (1974) (quoting Fuentes v. Shevin, 407 U.S. 67, 91 (1972)).

[221] *See supra* notes 152-66 and accompanying text.

[222] *See* Fort Wayne Books, Inc. v. Indiana, 489 U.S. 46, 63-64 (1989).

[223] *Id*.

[224] Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 657 (E.D. Pa. 2004).

probable cause is sufficient for the arrest of a person, but not for the seizure of First Amendment material.[225] Notwithstanding that edict, the DHS and DOJ seize and administratively forfeit domain names under the authority of the PRO-IP Act on the basis of nothing more than probable cause.[226] The practice and the law authorizing it are plainly in violation of the First Amendment.

Addressing the notice failure that occurs when domain names are seized ex parte is particularly important given the harmful and potentially far-reaching secondary effects of such seizures.[227] Ex parte domain name seizures potentially impact huge quantities of lawful third-party digital property and non-infringing speech, even in cases where the domain name registrants themselves turn out to be bad actors.[228] Through the civil forfeiture provisions in the PRO-IP Act, Congress empowered law enforcement agents to forego judicial process in order to increase the efficiency of anti-piracy operations; enhanced efficiency, however, cannot justify the abrogation of constitutional values and rights that are established in First and Fifth Amendment case law.[229]

An obvious policy solution to the constitutional infirmities inherent in the administrative forfeiture process is to codify the judicial holdings that limit ex parte seizures to provably exigent circumstances, and to require advance notice and a hearing in non-exigent cases. In cases involving domain names, even if exigent circumstances can be proven, probable cause is not a high enough standard where the purpose of the seizure is to remove expressive property from circulation. Legislation pending in the 114th Congress would raise the government's burden of proof in contested civil forfeiture proceedings from

[225] *See* United States v. Moore, 215 F.3d 681, 685 (7th Cir. 2000) ("While at first glance it may seem odd to require more judicial protection for the liberty of one's books than for one's body, the distinction reflects this country's great concern with the chilling effect on protected speech brought on by a government seizure.").

[226] *See supra* note 137 and accompanying text.

[227] Seizure of the mooo.com domain name in connection with a child pornography investigation in 2011 illustrates the potential magnitude of the problem. *See* Ted Samson, *Feds Wrongly Links 84,000 Seized Sites to Child Porn*, INFOWORLD (Feb. 17, 2011), http://www.infoworld.com/article/2623453/federal-regulations/feds-wrongly-links-84-000-seized-sites-to-child-porn.html [https://perma.cc/JB58-WNLG]. The government blocked access to 84,000 websites in an effort to seize ten domain names suspected of facilitating the distribution of illegal material. *Id*. ("[M]ooo.com isn't a domain used for anything related to child porn; rather, it's home to some 84,000 websites primarily belonging to individuals and small businesses.").

[228] *Cf*. Lizzie Plaugic, *Megaupload Copyright Infringement Case Sees Its First Conviction*, VERGE (Feb. 14, 2015, 4:37 PM), https://www.theverge.com/2015/2/14/8039413/megaupload-conviction-felony-nomm-kim-dotcom [https://perma.cc/C38F-YG2M] (reporting that one of Kim Dotcom's indicted, alleged co-conspirators—a programmer for Megaupload—reached a plea agreement with federal prosecutors in which he pled guilty to felony copyright infringement).

[229] *Cf*. Taylor v. Hayes, 418 U.S. 488, 500 (1974) ("Due process cannot be measured in minutes and hours or dollars and cents.").

preponderance of the evidence to clear and convincing evidence, and would require the government to prove that the property owner used the property with the intent to facilitate the alleged underlying offense.[230] These amendments would go a long way towards making the civil forfeiture process more consistent with due process across the board—for seizures of domain names and any other type of facilitation property. Additionally, to better protect the due process rights of innocent third parties who have a stake but no title in property the government proposes to seize, the innocent owner defense should be expanded to cover equitable as well as legal interests in forfeitable property.[231]

If the law is changed to require notice and a hearing before a domain name can be seized, willfully bad actors, many of whom operate from abroad, will be highly unlikely to appear in U.S. court to fight for their property. With or without notice, the bad actors will simply do what they do: play whack-a-mole, migrating illegal content to other domain names in top-level domains outside the in rem jurisdiction of U.S. law enforcement. In cases of mistake or law enforcement overreach, by contrast, legitimate registrants who get advance notice will have the opportunity they deserve to be heard in court before their property is taken and their online operations are disrupted, potentially irrecoverably. Fixing the notice failure inherent in ex parte domain name seizures will thus have no impact on the government's ability to shut down blatantly infringing sites whose owners have no interest in asserting their innocence. It will, however, prevent costly, careless mistakes by law enforcement in cases involving website owners who believe they are operating lawfully and would like to make that argument to a judge.

III. NAKED NOTICE: NONPARTY INJUNCTIONS IN "PIRATE SITE" CASES

Rule 65 of the Federal Rules of Civil Procedure governs the form and scope of injunctions and restraining orders in all civil cases, including those for copyright infringement.[232] Among other things, Rule 65 limits a court's power

[230] *See* Fifth Amendment Integrity Restoration Act (FAIR Act) of 2015, S. 255, 114th Cong. § 2 (2015) ("[I]f the Government's theory of forfeiture is that the property was used to commit or facilitate the commission of a criminal offense, or was involved in the commission of a criminal offense, the Government shall establish, by clear and convincing evidence, that . . . (B) the owner of any interest in the seized property (i) used the property with intent to facilitate the offense . . . ."); Fifth Amendment Integrity Restoration Act (FAIR Act) of 2015, H.R. 540, 114th Cong. § 2 (2015) (same).

[231] Prior to legislative amendments in 2000, which changed the scope of the innocent owner defense under federal civil forfeiture laws, courts recognized equitable interests in seized property as a basis for standing to challenge a forfeiture. *See, e.g.*, United States v. 74.05 Acres of Land, 428 F. Supp. 2d 57, 64-65 (D. Conn. 2006) (explaining that prior to enactment of the Civil Asset Forfeiture Reform Act, "an equitable interest recognized under state law was a sufficient ownership interest to grant a claimant standing as an innocent owner").

[232] FED. R. CIV. P. 65.

to enjoin persons not named as parties to litigation.[233] In a spate of recent copyright cases involving requests for site-blocking injunctions against "pirate sites," trial courts sympathetic to plaintiffs' whack-a-mole enforcement dilemma have taken a dubious shortcut around Rule 65. When granting motions for preliminary relief (either temporary restraining orders ("TROs") or preliminary injunctions) against offending website operators, courts invoking Rule 65—and, sometimes, a Delphic provision in federal law known as the All Writs Act—have overstepped the limits of their equitable powers by entering orders that name and impose obligations on whole categories of nonparty online intermediaries, including search engines, advertising networks, payment networks, domain name registrars, and operators of authoritative domain name servers.[234]

Expedient site-blocking injunctions against nonparty intermediaries implicate the third notice failure with which this article is concerned: the failure of some trial courts to appreciate their lack of jurisdiction to issue injunctions naming nonparties when those nonparties have had neither notice of the pending litigation nor an opportunity to be heard on the question of their relationship to the defendant's allegedly illegal acts. Online intermediaries are often in a technical position to effectuate orders against defaulting or uncooperative copyright defendants.[235] That capability, however, does not

[233] *See id*. 65(d)(2) ("The order binds only the following who receive actual notice of it by personal service or otherwise: (A) the parties; (B) the parties' officers, agents, servants, employees, and attorneys; and (C) other persons who are in active concert or participation with anyone described in Rule 65(d)(2)(A) or (B).").

[234] *See, e.g*., Elsevier Inc. v. www.Sci-Hub.org, No. 15 CIV. 4282(RWS), 2015 WL 6657363, at *6 (S.D.N.Y. Oct. 30, 2015) (granting a preliminary injunction that purported to bind "TLD Registries for the Defendants' websites"); Amended Preliminary Injunction at 2-4, ABS-CBN Int'l v. FreePinoyChannel.com, No. 15-61002-CIV-DIMITROULEAS/SNOW (S.D. Fla. July 28, 2015), ECF No. 30 (purporting to bind domain name registrars); Preliminary Injunction at 1, Arista Records, LLC v. Tkach, No. 1:15-CV-03701-AJN (S.D.N.Y. June 1, 2015), ECF No. 53 [hereinafter *Tkach* Preliminary Injunction] (purporting to bind "domain name registrars, domain name registries, and Internet service providers"); Order Granting Ex Parte Application for Entry of Temporary Restraining Order and Setting Hearing On Motion for Preliminary Injunction at 7-8, ABS-CBN Corp. v. Ashby, No. 3:14-cv-01275-HU (D. Or. Aug. 8, 2014) [hereinafter Order Granting TRO] (purporting to bind "any Internet search engines, Web hosts, domain-name registrars, and domain name registries or their administrators"); Preliminary Injunction at 2-3, Lions Gate Films Inc. v. John Does 1-10, No. 2:14-cv-06033-MMM-AGR (C.D. Cal. Aug. 8, 2014), ECF No. 28 [hereinafter *Lions Gate* Preliminary Injunction] (enjoining "persons and entities providing any services to or in connection with the domain names").

[235] *See, e.g*., JACQUELINE LIPTON, RETHINKING CYBERLAW: A NEW VISION FOR INTERNET LAW 4 (2015) ("Imposing injunctions on intermediaries to stanch harmful information flows will be much more effective than seeking relief against individuals often in multiple jurisdictions."); Jonathan Zittrain & John Palfrey, *Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 108 (Ronald Deibert et al. eds., 2008) ("The most salient form of filtering is

make intermediaries de facto aiders and abettors, nor does it give courts blanket equitable jurisdiction over them in cases where they can provide instant gratification for frustrated plaintiffs.[236] Copyright plaintiffs, like any others, are entitled to meaningful relief, including injunctive relief, but not at the expense of nonparties and their right to due process. Naked notice—mere notice of the existence of an injunction—is not enough to bind a nonparty service provider to the terms of the injunction.

A. *Rule 65, Piracy Panic, and Overreaching Injunctions*

As a general rule, a court has no authority to issue an order to a nonparty over whom it has not acquired personal jurisdiction.[237] The rationale for this limit on courts' jurisdiction lies in both due process and the separation of powers: courts are empowered to adjudicate disputes between parties before them and not to enact legislation for members of the general public.[238] Given that court orders are the law of the parties and not the law of the land, mere notice of the existence and contents of an injunction does not bind the world to its terms.[239]

Under Rule 65, a "[court] order binds only the following who receive actual notice of it by personal service or otherwise: (A) the parties; (B) the parties' officers, agents, servants, employees, and attorneys; and (C) other persons who are in active concert or participation with anyone described in . . . (A) or (B)."[240] The inclusion of those in active concert or participation with an enjoined party codifies the common law doctrine that an injunction binds both the defendants and "those identified with them in interest, in 'privity' with them, represented by them or subject to their control."[241] Within the meaning of Rule 65, a finding of privity sufficient to establish active concert between a nonparty and party is limited to circumstances in which the nonparty is so closely identified in interest with the defendant that it is reasonable to treat the

direct technical control implemented by legal controls trained on private actors who lie between an end-user and the network at large.").

[236] *Cf.* Doug Rendleman, *Beyond Contempt: Obligors to Injunctions*, 53 TEX. L. REV. 873, 933 (1975) ("Too frequently, a present emergency justifies a doubtful extension of equitable power that bends doctrine to fit that emergency.").

[237] *See* Additive Controls & Measurement Sys., Inc. v. Flowdata, Inc. (*Additive Controls I*), 96 F.3d 1390, 1394 (Fed. Cir. 1996) ("[A] court may not enter an injunction against a person who has not been made a party to the case before it."); Alemite Mfg. Corp. v. Staff, 42 F.2d 832, 832-33 (2d Cir. 1930) ("[A court] is not vested with sovereign powers to declare conduct unlawful; its jurisdiction is limited to those over whom it gets personal service, and who therefore can have their day in court.").

[238] *Additive Controls I*, 96 F.3d at 1394.

[239] *See Alemite Mfg. Corp.*, 42 F.2d at 832 ("[N]o court can make a decree which will bind anyone but a party; a court of equity is as much so limited as a court of law; it cannot lawfully enjoin the world at large, no matter how broadly it words its decree.").

[240] FED. R. CIV. P. 65(d)(2).

[241] Regal Knitwear Co. v. NLRB, 324 U.S. 9, 14 (1945).

nonparty's rights and interests as having been represented and adjudicated in the defendant's proceeding.[242] Another way of saying this is that the nonparty must have constructively had her day in court.[243] Mere contractual privity between a nonparty and the defendant is not the kind of close relationship that Rule 65 contemplates. For example, a nonparty distributor of patent-infringing wrenches was held not to be in Rule 65 privity with the defendant manufacturer, with which the distributor had multiple contracts relating to sale of the wrenches, because the two were "distinct entities involved in arm[']s length transactions."[244]

There are two senses in which a nonparty "in active concert or participation with" a defendant can be bound by an injunction against that defendant: she can be bound as one who acted in concert with the defendant in the illegal conduct alleged in the complaint, or she can be bound as one who subsequently acted in concert with the defendant to violate the injunction.[245] In the latter scenario, she is a contemnor, and the injunction is enforceable against her through the court's contempt jurisdiction.[246] Before a nonparty can be *named* in an injunction as one who is in active concert with the defendant, due process requires evidence of the requisite relationship of complicity between the nonparty and the defendant.[247] The same is true for a finding of contempt against a nonparty *not named* in an injunction who, after the injunction issues,

[242] Harris Cty. v. CarMax Auto Superstores Inc., 177 F.3d 306, 314 (5th Cir. 1999).

[243] *Id*.

[244] Petersen v. Fee Int'l, Ltd., 435 F. Supp. 938, 944 (W.D. Okla. 1975).

[245] Doug Rendleman has argued perceptively that the rubrics of "parties/nonparties" and "bound/not bound," which tend to dominate discussions on the scope of injunctions, are unhelpful for answering the "who-must-obey" question. Rendleman, *supra* note 236, at 876. He refers to non-litigants who are not named in an injunction, but who may be held guilty of contempt, as "potential contemnors." *Id*. Such persons are "parties" to the injunction, in the sense that they must "obey it or be subject to contempt," but they are not "parties" to the underlying litigation, because they were not served and did not litigate. *Id*. Potential contemnors will be actual contemnors in Rendleman's parlance only if they are found to be "obligors" by virtue of having the requisite relationship to the defendant. *See id*. at 877 ("Unless the potential contemnor is also an obligor, he may ignore the injunction with impunity.").

[246] *Cf*. 11A CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 2956 (3d ed. 2013) (explaining that nonparties who are not in privity with any parties may not be brought within the effect of an injunction merely by naming them in the order, but that nonparties with actual notice of a court order who aid and abet the defendant in violating it may be held in contempt).

[247] *See* Zenith Radio Corp. v. Hazeltine Research, Inc., 395 U.S. 100, 112 (1969) (holding that it was error for a court to enter an injunction against a nonparty corporation that was allegedly the alter ego of the defendant without having made that determination in a proceeding to which the alleged alter ego was a party).

allegedly aids and abets the defendant in violating the injunction.[248] In both situations, the law requires not only notice of the injunction, but also an opportunity for the nonparty to be heard on the issue of active concert.[249] The fact that a court asserts in an order that a nonparty is bound does not make it so. As the Supreme Court held in *Regal Knitwear Co. v. NLRB*, whether a nonparty is subject to an injunction "depends on an appraisal of his relations and behavior and not upon mere construction of terms of the order."[250]

Courts interpret Rule 65's "active concert or participation" standard in the same way they do the aiding and abetting standard in criminal law.[251] A person does not aid and abet merely by associating herself with a venture; she must participate in the venture actively with a desire to see it succeed.[252] Under the criminal aiding and abetting cases, knowledge that one is participating in an illegal transaction is an essential element of the offense.[253] Merely being "a knowing spectator," however, is not enough to establish aiding and abetting.[254] To abet illegal activity, a person must have, in Learned Hand's words, a "purposive attitude towards it."[255]

An illustrative case is *United States v. Martiarena*.[256] The defendant was an unpaid employee of her father's "currency exchange house" in Texas, near the U.S.-Mexico border.[257] She was accused of aiding and abetting her father in his willful failure to file a Currency Transaction Report ("CTR") documenting the

[248] *See* Vuitton et Fils S.A. v. Carousel Handbags, 592 F.2d 126, 130 (2d Cir. 1979) (requiring an evidentiary hearing to determine whether nonparties alleged to be aiders and abettors of the enjoined defendant, a counterfeit handbag retailer, had the requisite relationship with the retailer to be held in contempt for violating the injunction against it).

[249] *See, e.g.*, *id*.

[250] Regal Knitwear Co. v. NLRB, 324 U.S. 9, 15 (1945).

[251] *See* Blockowicz v. Williams, 630 F.3d 563, 567 (7th Cir. 2010) ("Consistent with this purpose, we have explained that a person is in 'active concert or participation' with an enjoined party, and thus bound by the injunction, if 'he aids or abets an enjoined party in violating [the] injunction,' or if he is in privity with an enjoined party." (quoting Nat'l Spiritual Assembly of the Bahá'ís of the U.S. Under the Hereditary Guardianship, Inc., v. Nat'l Spiritual Assembly of the Bahá'ís of the U.S., Inc., 628 F.3d 837, 848 (7th Cir. 2010))); *see also* Petersen v. Fee Int'l, Ltd., 435 F. Supp. 938, 944 (W.D. Okla. 1975) ("The active concert and participation language of Rule 65 clearly is derived from the common law aiding and abetting concept.").

[252] Nye & Nissen v. United States, 336 U.S. 613, 619 (1949).

[253] *E.g.*, United States v. Moody, 462 F.2d 1307, 1308 (8th Cir. 1972).

[254] United States v. Dixon, 658 F.2d 181, 189-90 (3d Cir. 1981) (quoting United States v. Rosa, 404 F. Supp. 602, 617 (W.D. Pa. 1975), *aff'd*, 560 F.2d 149 (3d Cir. 1977)) (affirming a jury finding of aiding and abetting where the defendant not only knew of the bribery scheme in question, but also "agreed to the plan's terms and gave his assurance that he would take care of his 'side of the business'").

[255] United States v. Peoni, 100 F.2d 401, 402 (2d Cir. 1938).

[256] 955 F.2d 363 (5th Cir. 1992).

[257] *Id*. at 364-65.

exchange from dollars to pesos of more than $10,000 in cash.[258] A jury convicted her on the basis that she assisted in the underlying transaction.[259] The district court reversed the verdict and ordered a judgment of acquittal.[260] In affirming the district court's judgment, the Fifth Circuit held that the government failed to prove that the defendant shared her father's willful intent or actively contributed to his not filing the required form.[261] The court pointed out that different facts might have led to a different result: "Had she lied about the amount involved, given assurances that no CTR would be filed, or otherwise actively aided her father's failure, a different case would have been presented."[262] As the facts stood, however, the panel agreed with the district court's conclusion that the government failed to carry its burden of proving both that the defendant shared her father's criminal intent and that she engaged in affirmative conduct to assist him in or reward him for violating the law.[263]

The school desegregation cases of the 1970s represent what is probably the most liberal—and marginal—application of Rule 65's provisions governing judicial power over nonparties. In *United States v. Hall*,[264] the Fifth Circuit upheld a district court's very broad injunction against nonparty protesters who joined with African American students and their parents in boycotts and other activities intended to prevent the normal operation of a recently integrated Florida high school.[265] In the underlying civil rights litigation, *Mims v. Duval County School Board*, a district court ordered the defendant school board to desegregate the schools under its control by pairing schools that had been predominantly one-race schools and transferring students between them to integrate their respective student bodies.[266] After the school board acted to comply with the order, racial unrest erupted at one of the schools.[267] The superintendent petitioned the *Mims* court, which had retained jurisdiction in the case, for an injunction against all persons "interfering with the orderly operation of the school."[268] The court granted the petition and entered an

[258] *Id*. at 364-66.

[259] *See id*. at 366-67 ("The necessary inquiry then must be whether the telephone call she placed to her father to inform him that the [undercover] agents were at the Texaco casa to see him, her call to her boyfriend to meet her father to help transport the pesos into the United States, and her waiting at the casa with the agents pending her father's return on March 8, 1989, constituted 'participation' in her father's subsequent and independent failure to file the required CTR.").

[260] *Id*. at 366.

[261] *See id*. at 366-67.

[262] *Id*. at 367.

[263] *Id*. at 366-67.

[264] 472 F.2d 261 (5th Cir. 1972).

[265] *Id*. at 262-64.

[266] *See id*. at 262-63.

[267] *Id*. at 263.

[268] *Id*.

injunction that named Hall and six others.[269] Hall challenged the order on the ground that he was not a party to *Mims*, was acting independently of the parties, and was therefore beyond the court's injunctive power.[270]

In its opinion rejecting Hall's challenge, the Fifth Circuit went out of its way to emphasize the "peculiar problems" caused by school desegregation cases.[271] The court pointed out that the enjoined nonparty activity, if it had *not* been prohibited by the district court, would have effectively prevented both the plaintiffs from exercising their constitutional rights and the defendant from performing its constitutional duty as the *Mims* court had ordered.[272] Given the symbolism and magnitude of the underlying litigation, *Hall* is best understood as an exceptional case in which the court's exercise of jurisdiction over nonparties was upheld because those nonparties were willfully and actively interfering with the parties as they attempted in good faith to comply with a court order of historic significance. Considering the historical context, *Hall* and its ilk should not be viewed as generally applicable precedents when it comes to the reach of a court's power under Rule 65 over independent nonparty actors.

Ignoring the behavioral and relational standards for determining active concert, federal district courts in recent "pirate site" cases have been ordering injunctive relief against a slew of independent nonparty service providers. Federal district courts in Oregon and Florida issued ex parte TROs in a pair of cases brought by a Philippine production company and its California affiliate.[273] The defendants in these cases were accused of operating about two dozen "pirate websites" that infringed the plaintiffs' copyrights in movies and TV shows for Filipino audiences.[274] In addition to ordering the defendants to stop engaging in infringing conduct, the courts ordered "those with actual notice of the injunction, including any Internet search engines, Web hosts, domain-name registrars, and domain name registries or their administrators [to] cease facilitating access to any or all domain names and websites through which Defendants engage in the [infringement] of Plaintiffs' copyrighted works."[275] Both courts ordered the domain name registrars that had originally

[269] *Id*.

[270] *Id*. at 264.

[271] *Id*. at 266.

[272] *Id*. at 265 ("Disruption of the orderly operation of the school system, in the form of a racial dispute, would thus negate the plaintiffs' constitutional right and the defendant's constitutional duty. In short, the activities of persons contributing to racial disorder at Ribault imperiled the court's fundamental power to make a binding adjudication between the parties properly before it.").

[273] Amended Preliminary Injunction, *supra* note 234; Order Granting TRO, *supra* note 234.

[274] Amended Preliminary Injunction, *supra* note 234; Order Granting TRO, *supra* note 234.

[275] *See, e.g.*, Order Granting TRO, *supra* note 234, at 7-8. The TROs in the two cases appear to be identical in their language and scope.

registered the defendants' domain names to transfer the registrations for the pendency of the litigation to new registrars chosen by the plaintiffs.[276] They then ordered the new, as-yet-unidentified registrars to divert traffic from the defendants' sites to a location displaying legal documents from the case.[277] None of the online intermediaries targeted by the orders was a named party in either case, and none had been accused in the complaints of violating the law or any previously issued court order against the defendants.

A federal district court in California issued a TRO, followed shortly thereafter by a preliminary injunction, in a case involving websites streaming and distributing pre-release copies of the movie "The Expendables 3."[278] The California court's order was both sweeping and completely conclusory in its identification of nonparties in active concert or participation with the defendants. The injunction encompassed "persons and entities providing any services to or in connection with the domain names <limetorrents.com>, <billionuploads.com>, <hulkfile.eu>, <played.to>, <swankshare.com> and/or <dotsemper.com> or the websites to which any of those domain names resolve."[279] In addition to domain name registrars and hosting services, the court's order swept in "[a]ll banks, savings and loan associations, payment processors or other financial institutions, payment providers, third party processors and advertising service providers of Defendants."[280] None of the online intermediaries targeted in the order was a named party in the case, none was accused of illegal conduct in the complaint, and none was accused of violating any previously issued court order against the defendants.

A district court in New York was similarly obliging to plaintiffs in a case involving domain name copycats of the shuttered music streaming site Grooveshark.com.[281] In two separate actions, the major recording labels won summary judgment against Grooveshark's operator, Escape Media, for copyright infringement.[282] At the conclusion of those cases, Escape Media

[276] Amended Preliminary Injunction, *supra* note 234, at 2; Order Granting TRO, *supra* note 234, at 8.

[277] Amended Preliminary Injunction, *supra* note 234, at 3; Order Granting TRO, *supra* note 234, at 9.

[278] Temporary Restraining Order and Order to Show Cause Why a Preliminary Injunction Should Not Issue, Lions Gate Films Inc. v. John Does 1-10, No. 2:14-cv-06033-MMM-AGR (C.D. Cal. Aug. 4, 2014), ECF No. 17. The court entered the preliminary injunction four days after the issuance of the TRO, on August 8. *Lions Gate* Preliminary Injunction, *supra* note 234.

[279] *Lions Gate* Preliminary Injunction, *supra* note 234, at 2.

[280] *Id*. at 3-4.

[281] Arista Records, LLC v. Tkach, No. 1:15-CV-03701 (AJN), 2015 WL 4743756, at *1 (S.D.N.Y. June 3, 2015). The court entered a preliminary injunction in the case on June 1, 2015. *Id*.

[282] Capitol Records, LLC v. Escape Media Grp., Inc., No. 12-CV-6646 (AJN), 2015 U.S. Dist. LEXIS 38007, at *2 (S.D.N.Y. Mar. 25, 2015); UMG Recording v. Escape Media Grp., No 11 Civ. 8407, 2014 U.S. Dist. LEXIS 137491, at *3 (S.D.N.Y. Sept. 29, 2014).

transferred Grooveshark's federally registered trademarks to the plaintiffs as part of a permanent injunction and consent judgment.[283] Shortly after entry of the consent judgment, unknown persons registered the Grooveshark domain name in two other top-level domains—.io and .pw, which are the country code Top Level Domains ("ccTLDs") for the British Indian Ocean Territory and Palau, respectively.[284] The anonymous registrants of the copycat sites appeared to be offering the same unauthorized content for which Escape Media had been found liable.[285] Arista and its co-plaintiffs lost no time in moving for a TRO and filing suit for copyright and trademark infringement against the John Doe registrants of the copycat sites.[286] The labels' lawyers succeeded in shutting down the .io and .pw sites, but other "clones" cropped up in different ccTLDs.[287]

As in the cases described above, no domain name registrars or ISPs were parties to the Grooveshark copycat litigation, and none had notice that the plaintiffs were seeking to include them within the scope of preliminary injunctions. The plaintiffs sought and won a TRO that purported to bind "any persons acting in concert or participation with [Defendants] *or* third parties providing services used in connection with Defendants' operations," *or* having knowledge of the order.[288] By its terms, the TRO—like those issued in the Florida and Oregon cases[289]—covered not only nonparties in active concert with the defendants *and* having notice of the order, as permitted by Rule 65, but also any nonparties providing services to the defendants or simply having notice of the order. The order was thus plainly overbroad.[290] The court later entered a preliminary injunction, which was somewhat less inclusive in its language, but still purported to bind nonparty "domain name registrars, domain name registries, and Internet service providers," all of whom the order conclusorily characterized as being in active concert with the defendant.[291]

The pattern that emerges from these cases is one in which copyright plaintiffs who are frustrated by the difficulty of enforcing their rights online

[283] *See Tkach*, 2015 WL 4743756, at *1.

[284] *Id*. at *1-2.

[285] *See* Jacob Kastrenakes, *A New Grooveshark Is Online and Streaming Music*, THE VERGE (May 5, 2015, 4:46 PM), https://www.theverge.com/2015/5/5/8555327/grooveshark-clone-revives-music-streaming-site [https://perma.cc/MB6Q-LSCA] (reporting on the operation of the purported clone site at www.grooveshark.io).

[286] *See Tkach*, 2015 WL 4743756, at *1 (stating that a judge entered a temporary restraining order on May 13, 2015, and that the court entered a preliminary injunction on June 1, 2015).

[287] *Id*. at *2.

[288] *Id*. at *1 (emphasis added).

[289] *See supra* note 275 and accompanying text.

[290] *See, e.g.*, Chase Nat'l Bank v. City of Norwalk, 291 U.S. 431, 436 (1934) ("[T]he decree entered by the District Court was clearly erroneous in so far as it enjoined 'all persons to whom notice of the order of injunction should come . . . .'").

[291] *Tkach* Preliminary Injunction, *supra* note 234, at 1.

successfully persuade judges to grant them orders to which they are not legally entitled against nonparties over whom the courts lack jurisdiction. The affected nonparties, moreover, are assumed to be aiders and abettors without the necessary factual showing of active complicity in the defendants' alleged illegal conduct—either pre-complaint or post-injunction.[292] As the Seventh Circuit held in *Blockowicz v. Williams*,[293] "the fact that [a nonparty service provider] is technologically capable of removing [content] does not render its failure to do so aiding and abetting" for the purpose of establishing contempt jurisdiction.[294] Moreover, unlike the enjoined nonparties in *Hall*, who actively interfered with the defendant's ability to comply with a court order, the nonparty intermediaries in the copyright cases discussed above in no way interfered with or thwarted any efforts of the defendant site operators to comply with court orders directing them to stop infringing.[295] The defendants were often non-compliant, but their noncompliance was neither solicited nor caused by the online service providers. It is true, as the saying goes, that equity will not suffer a wrong without a remedy.[296] That is not to say, however, that a court's equitable powers are unlimited, especially where the fundamental rights and interests of nonparties are implicated in the court's remedial inclinations.[297]

B. *The All Writs Act and Its Limits in Copyright Cases*

In addition to citing Rule 65, some courts granting broad preliminary orders against nonparties in "pirate site" cases have cited the All Writs Act as a source of authority. As succinct as it is vague, the All Writs Act provides that

[292] *See Chase Nat'l Bank*, 291 U.S. at 441 ("Unless duly summoned to appear in a legal proceeding, a person not a privy may rest assured that a judgment recovered therein will not affect his legal rights.").

[293] 630 F.3d 563 (7th Cir. 2010).

[294] *Id.* at 568.

[295] Because domain name registrants (i.e., website operators) have direct control over the content available through their websites, they have the power to eliminate infringing content. Domain name intermediaries have no control over the content available on websites. *Cf.* Globalsantafe Corp. v. Globalsantafe.com, 250 F. Supp. 2d 610, 619 (E.D. Va. 2003) (explaining what domain name registrars and registry operators do and how they function).

[296] Indep. Wireless Tel. Co. v. Radio Corp. of Am., 269 U.S. 459, 472 (1926).

[297] One commentator has recommended an amendment to Rule 65 that would have the effect of binding nonparty search engines to injunctions ordered against infringing domain names. *See* Courtney Brown, *Caught in a Bind: Reassessing Judicial Authority to Bind Non-Party Search Engines Under Rule 65 in Counterfeit Goods Cases*, 32 CARDOZO ARTS & ENT. L.J. 257, 280-81 (2013). She would relax the active concert requirement to include those who "involuntarily 'enable'" unlawful conduct. *Id.* at 260. Such a broad expansion of the equitable powers of courts in all civil cases would doubtless have unintended costs and consequences far beyond search engines and the realm of online intellectual property enforcement.

"[t]he Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[298] On its face, the Act appears to give courts supplemental injunctive powers beyond what Rule 65 allows, but the case law clearly establishes that the provision is not a grant of independent jurisdiction to the federal courts.[299]

One key to understanding the proper bounds of the All Writs Act is parsing what it means for a court to act "in aid of its jurisdiction." Courts interpreting the All Writs Act have construed the statute's "in aid of jurisdiction" language to mean that a court's power under the Act is "limited . . . to the facilitation of the court's effort to manage [a] case to judgment"[300] or "to control actions or conduct that would inhibit its ability to resolve or manage a case before it."[301] For example, courts have permissibly used the All Writs Act to enjoin a nonparty's dissipation of funds potentially subject to a constructive trust at the conclusion of litigation[302] and to prevent the consummation of a merger that the FTC was preparing to challenge and that, if completed, would have been impervious to remedial measures.[303] Courts have also used the Act to enjoin duplicative proceedings in a state court that could have negatively impacted settlement negotiations in a parallel federal class action,[304] to permit the use of interrogatories in habeas corpus proceedings,[305] and to aid in conducting factual inquiries necessary to the resolution of a case.[306]

---

[298] 28 U.S.C. § 1651 (2012).

[299] *See* Gen. Bldg. Contractors Ass'n, Inc. v. Pennsylvania, 458 U.S. 375, 402 (1982) (holding that injunctive relief under the All Writs Act was improper where the enjoined nonparties "could not properly be held liable to any sort of injunctive relief based on their own conduct"); *In re* "Agent Orange" Prod. Liab. Litig., 996 F.2d 1425, 1431 (2d Cir. 1993) ("[T]he All Writs Act is not a jurisdictional blank check."), *overruled in part by* Syngenta Crop Prot., Inc. v. Henson, 537 U.S. 28 (2002); United States v. Int'l Bhd. of Teamsters, 907 F.2d 277, 281 (2d Cir. 1990) (holding that the All Writs Act authorizes injunctions against nonparties only to protect the court's jurisdiction, and "does not enlarge the jurisdiction of the federal courts"); Fla. Med. Ass'n, Inc. v. U.S. Dept. of Health, Ed. & Welfare, 601 F.2d 199, 202 (5th Cir. 1979) ("[T]he All Writs Act does not free a district court from the restraints of Rule 65.").

[300] ITT Cmty. Dev. Corp. v. Barton, 569 F.2d 1351, 1359 (5th Cir. 1978).

[301] Cinel v. Connick, 792 F. Supp. 492, 497 (E.D. La. 1992).

[302] *See Barton*, 569 F.2d at 1351, 1359 ("[T]he All Writs Act could have served as authority for the turn-over order here in question only to curb conduct which threatened improperly to impede or defeat the subject matter jurisdiction then being exercised by the court.").

[303] FTC v. Dean Foods Co., 384 U.S. 597, 605 (1966).

[304] Carlough v. Amchem Prods., Inc., 10 F.3d 189, 201-04 (3d Cir. 1993).

[305] Harris v. Nelson, 394 U.S. 286, 288, 299 (1969).

[306] *See* American Lithographic Co. v. Werckmeister, 221 U.S. 603, 608-10 (1911).

In *United States v. New York Telephone Co.*,[307] a deeply divided opinion testing the limits of judicial authority under the All Writs Act, the Supreme Court upheld an injunction ordering a nonparty telephone company to assist the government in installing a pen register on the telephone company's property, in furtherance of a law enforcement investigation.[308] In a lengthy dissent, Justice Stevens (joined by Justices Marshall, Brennan, and Stewart) faulted the majority for conflating "the District Court's interest in its jurisdiction . . . with the Government's interest in a successful investigation."[309] Citing precedent in which the Court overturned a trial court injunction requiring the Civil Service Commission to reinstate a fired employee, Justice Stevens asserted that aiding a party in effectuating its rights or duties is not a sufficient basis for granting a writ under the Act.[310] "[C]ourts," he wrote, "have consistently recognized and applied the limitation that whatever action the court takes must be in aid of *its* duties and *its* jurisdiction," not in aid of a remedy for an aggrieved party.[311] At the conclusion of his dissent, Justice Stevens characterized the order in the case as a "deeply troubling . . . portent of the powers that future courts may find lurking in the arcane language of . . . the All Writs Act."[312] Courts in pirate site cases have fulfilled his prophecy, exercising their powers under the Act to conscript independent nonparties without consent or due process, to assist plaintiffs in getting expedient, workaround remedies when adjudicated infringers ignore court orders.[313]

A second key to understanding the limits of judicial power under the All Writs Act is the rule that statutory injunction provisions completely displace it.[314] The Supreme Court has said that "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute."[315] In cases where a statute is responsive to the issue before the court, the statute, not the All Writs Act, controls the nature and scope of the court's order.[316] In a given

[307] 434 U.S. 159 (1977).

[308] *Id.* at 168, 172, 175.

[309] *Id.* at 190 (Stevens, J., dissenting). The majority found this distinction to be "specious." *Id.* at 175 n.23 (majority opinion).

[310] *Id.* at 189 (Stevens, J., dissenting) (citing Sampson v. Murray, 415 U.S. 61 (1974)).

[311] *Id.*

[312] *Id.* at 191.

[313] *Cf. Additive Controls I*, 96 F.3d 1390, 1397 (1996) ("Although an injunctive order prohibiting non-parties from disposing of [patent-infringing devices] may be more efficient than a separate lawsuit against those parties, the All Writs Act does not authorize that kind of adjudicative shortcut.").

[314] *Cf.* FTC v. Dean Foods Co., 384 U.S. 597, 622 (1966) ("The Act is abused where . . . it is contorted to confer jurisdiction where Congress has plainly withheld it.").

[315] Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 43 (1985).

[316] *See id.* ("Although the Act empowers federal courts to fashion extraordinary remedies when the need arises, it does not authorize them to issue ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate.").

case, the question to be answered is whether the plaintiff is asking the court to fill in a statutory gap that Congress failed to consider, or instead is asking the court to exercise authority that Congress chose not to confer.[317] A court may invoke the All Writs Act to do the former, but not the latter.

Anyone reading the All Writs Act cases in tandem with the provisions of the Copyright Act governing injunctions would be hard-pressed to conclude that the All Writs Act is a legitimate basis for the injunctions issued in the cases discussed above. The injunction provisions in the Copyright Act are designed to reach copyright infringers.[318] Under § 502, the court may "grant temporary and final injunctions on such terms as it may deem reasonable to prevent or restrain infringement of a copyright."[319] Under § 503, as discussed in Section II.A above, a court may order the impoundment of infringing articles in a pending case and the destruction of those articles at the case's conclusion.[320] Courts in copyright cases have broad discretion over whether to issue injunctions, but "such relief is not granted where the addressee of the injunction has not violated the plaintiff's copyrights and is not likely to do so in the future."[321] For example, a nonparty purchaser of an infringing copy of a book cannot be ordered to surrender the book, even though surrendering the book would mitigate the effect of the copyist's infringement.[322]

The DMCA contains a special injunction provision for online service providers.[323] That provision, § 512(j), governs applications under § 502 for injunctions against service provider defendants who qualify for safe harbor from money damages for their users' infringements.[324] The language of

[317] *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 1:15-mc-01902-JO, 2015 WL 5920207, at *1 (E.D.N.Y. Oct. 9, 2015).

[318] Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 433-34 (1984) ("The Copyright Act provides the owner of a copyright with a potent arsenal of remedies against *an infringe*r of his work, including an injunction to restrain *the infringer* from violating his rights . . . ." (emphasis added)).

[319] 17 U.S.C. § 502(a) (2012).

[320] *Id*. § 503.

[321] Societe Civile Succession Richard Guino v. Int'l Found. for Anticancer Drug Discovery, 460 F. Supp. 2d 1105, 1110 (D. Ariz. 2006); *see also* Paramount Pictures Corp. v. Carol Publ'g Grp., Inc., 25 F. Supp. 2d 372, 376 (S.D.N.Y. 1998) (denying the plaintiff's request to require the defendant publisher to notify nonparty booksellers that they were bound by the injunction against the publisher because the plaintiff failed to show that the booksellers were in "active concert or participation" with the publisher).

[322] *See Societe Civile*, 460 F. Supp. 2d at 1111-12 (holding that § 503 "does not permit the impoundment of infringing items in the hands of innocent purchasers who are not themselves liable for infringement").

[323] *See* 17 U.S.C. § 512(j) (governing "any application for an injunction under section 502 against a service provider that is not subject to monetary remedies under this section").

[324] *Id*. ("With respect to conduct other than that which qualifies for the limitation on remedies set forth in subsection (a), the court may grant injunctive relief with respect to a

§ 512(j) takes for granted that a covered service provider has successfully asserted one or more of the DMCA safe harbors as an affirmative defense in litigation to which the provider was a party. The provision therefore does not contemplate injunctive relief against nonparty service providers. Moreover, § 512(j) expressly requires notice to the affected service provider and an opportunity for the provider to be heard prior to the grant of an injunction.[325]

In 2011, Congress considered legislation that would have expanded courts' injunctive powers over online intermediaries in copyright cases to include site-blocking orders against a wide range of service providers, such as search engines, advertising networks, payment networks, and domain name registrars and registries.[326] The two bills, the Stop Online Piracy Act ("SOPA") and the PROTECT-IP Act ("PIPA"), were abandoned after an unprecedented public revolt over their likely consequences for the Internet's technical infrastructure and its speech-proliferating culture.[327] The service providers that would have been covered by the site-blocking provisions in SOPA and PIPA, had they become law, are the same ones covered by the nonparty injunctions issued in the cases discussed above. In these cases, courts are using their equitable powers under the All Writs Act to do quietly what Congress very noisily declined to do when it shelved SOPA and PIPA: compel neutral intermediaries operating at arm's length from accused infringers to implement court-ordered site-blocking. Because the court orders in these cases contravene the intent of Congress with respect to the availability of injunctive relief against online intermediaries, the All Writs Act cannot authorize them, no matter how convenient they are for plaintiffs.[328]

service provider only in one or more of the following forms: (i) an order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network . . . .").

[325] *Id*. § 512(j)(3) ("Injunctive relief under this subsection shall be available only after notice to the service provider and an opportunity for the service provider to appear are provided, except for orders ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider's communications network.").

[326] *See, e.g*., Stop Online Piracy Act (SOPA), H.R. 3261, 112th Cong. (2011) (requiring various types of service providers to "take technically feasible and reasonable measures" to withhold services from "foreign infringing sites" and to prevent users in the United States from accessing the allegedly infringing material on those sites). The range of providers that would have been covered by SOPA and PIPA was wider than the range eligible for safe harbor under § 512. *See* 17 U.S.C. § 512(k).

[327] *See* Annemarie Bridy, *Copyright Policymaking as Procedural Democratic Process: A Discourse-Theoretic Perspective on ACTA, SOPA, and PIPA*, 30 CARDOZO ARTS & ENT. L.J. 153 (2012) (explaining the controversy over SOPA and PIPA and the public outcry they precipitated).

[328] These cases differ in this important respect from *United States v. New York Telephone Co*., discussed above, in which the Supreme Court upheld an All Writs Act injunction ordering a nonparty telecommunications provider to install a pen register at its facility to aid

C. *Fixing the Failure: Aligning Judicial Reach with Judicial Grasp*

Fixing the notice failure associated with overreaching injunctions in "pirate site" cases requires courts to understand the proper scope of copyright injunctions against nonparty service providers. The All Writs Act is not a legitimate source of judicial power in these cases because no legislative gap exists for the courts to fill with respect to the kinds of injunctive relief available to plaintiffs in copyright cases.[329] With respect to Rule 65, courts must realize that notice of an injunction on its own is not sufficient to bind a nonparty service provider to its terms. Moreover, the due process problems associated with naked notice are not cured by conclusory statements in a court order about the complicity of nonparty service providers in a defendant's bad acts. Nonparty service providers have a right to be heard on the issue of active concert before they are brought within the scope of a preliminary injunction, either as an initial matter or through a contempt proceeding.[330]

At both junctures in the litigation, aggrieved rights holders seeking injunctive relief bear an evidentiary burden with respect to the alleged active concert of a nonparty service provider.[331] It offends due process for a court to regard the arm's length provision of technical services to an infringer as aiding and abetting per se. Giving meaningful content to aiding and abetting requires courts to remember that Rule 65, on its face, requires active *concert* with an enjoined defendant. "Concert" has an established common law meaning that

in an FBI investigation. *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 161 (1977). The majority in *New York Telephone Co*. examined the legislative history of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to determine whether Congress intended to bring pen registers within the scope of the statute, thereby depriving courts of jurisdiction under the All Writs Act to order their installation. *Id*. at 165-68. Quoting language from a Senate Report explaining that the statute's definition of "intercept" was purposely drafted to *exclude* pen registers, and to cover only the contents of communications, the majority concluded that Congress did not intend to regulate the use of pen registers in Title III. *Id*. On the contrary, the majority pointed out, the Senate Report stated explicitly that "[t]he use of a 'pen register,' . . . would be permissible." *Id*. at 167.

It may be argued that congressional intent should not be inferred from the fact that proposed legislation failed to pass. In the case of SOPA and PIPA, however, the debates over the legislation inside and outside Congress were reported extensively in the national media, and the public record is therefore full of evidence of both legislative and executive intent to reject the service-provider injunctions that the legislation would have permitted. *See* Bridy, *supra* note 327.

[329] *See supra* notes 314-17 and accompanying text.

[330] *See* Microsystems Software, Inc. v. Scandinavia Online AB, 226 F.3d 35, 43 (1st Cir. 2000) ("A nonparty who has acted independently of the enjoined defendant will not be bound by the injunction, and, if she has had no opportunity to contest its validity, cannot be found in contempt without a separate adjudication.").

[331] *Cf., e.g*., Zenith Radio Corp. v. Hazeltine Research, Inc., 395 U.S. 100, 112 (1969) ("[A] nonparty with notice cannot be held in contempt until shown to be in concert or participation.").

should serve as a guide in cases involving nonparty injunctions.[332] It requires, first among other elements, an express or tacit agreement to participate in a common plan or design to commit a tortious act.[333] This amounts, as courts in Rule 65 cases have held, to acting in collusion with or as an alter ego of the defendant.[334]

Guided by the common law criterion of an agreement to further a common tortious purpose, courts deciding whether nonparty service providers are acting in concert with their infringing customers for Rule 65 purposes should eschew the fast and loose understanding of aiding and abetting that copyright plaintiffs in "pirate site" cases are advocating. In keeping with a more rigorous definition of concert, courts must require copyright plaintiffs to show that the nonparty service providers they seek to enjoin have either expressly or tacitly agreed to act in furtherance of a common plan of infringement. In cases involving allegations of contempt, courts must require the plaintiff to show an express or tacit agreement between the service provider and the defendant to violate an injunction prohibiting the defendant from infringing.[335] Absent an affirmative showing of both common design and knowing participation in infringing (or injunction-violating) acts, a court cannot hold that a nonparty service provider is bound by an injunction without violating that service provider's due process rights.[336]

---

[332] *See* RESTATEMENT (SECOND) OF TORTS § 876 cmt. a (AM. LAW INST. 1979) ("Parties are acting in concert when they act in accordance with an agreement to cooperate in a particular line of conduct or to accomplish a particular result. The agreement need not be expressed in words and may be implied and understood to exist from the conduct itself. Whenever two or more persons commit tortious acts in concert, each becomes subject to liability for the acts of the others, as well as for his own acts. The theory of the early common law was that there was a mutual agency of each to act for the others, which made all liable for the tortious acts of any one.").

[333] *See, e.g.*, Pittman by Pittman v. Grayson, 149 F.3d 111, 122 (2d Cir. 1998) (stating the three elements of concerted-action liability in torts: "(1) an express or tacit agreement 'to participate in a common plan or design to commit a tortious act,' (2) tortious conduct by each defendant, and (3) the commission by one of the defendants, in pursuance of the agreement, of an act that constitutes a tort" (quoting Rastelli v. Goodyear Tire & Rubber Co., 591 N.E.2d 222, 224 (N.Y. 1992))); *see also supra* notes 251-55 and accompanying text.

[334] Thaxton v. Vaughan, 321 F.2d 474, 478 (4th Cir. 1963); *see also* United Pharmacal Corp. v. United States, 306 F.2d 515, 518 (1st Cir. 1962) (holding that a nonparty was not in active concert or participation in violating an injunction where it was not identified with the defendant "in the sense of being its agent, servant, subsidiary, tool, cat's paw or alter ego").

[335] *Cf.* Blockowicz v. Williams, 630 F.3d 563, 568 (7th Cir. 2010) (holding that there was no showing of aiding and abetting where the plaintiffs failed to present evidence that the nonparty service providers "had any contact with the defendants after the injunction was issued, or that they worked in concert with the defendants to violate the injunction").

[336] *See* Alemite Mfg. Corp. v. Staff, 42 F.2d 832, 833 (2d Cir. 1930) ("[T]he only occasion when a person not a party may be punished, is when he has helped to bring about,

Courts understandably want to do equity in cases involving brazen infringers like the Grooveshark copycats. And beleaguered rights holders understandably want to find creative solutions to the seemingly intractable problem such defendants pose. Both judges and rights holders must recognize, however, that equitable remedies implicating nonparties not afforded due process undermine the credibility of the courts and the integrity of judicial process. In that respect, they do more systemic harm than localized good.

CONCLUSION

Peter Menell and Michael Meurer have explored the negative consequences of notice failures as they relate to the scope of intellectual property entitlements.[337] This article turns to the enforcement side of the equation, examining notice failures embedded in legal efforts to control online copyright piracy. Two of the three notice failures this article examines—uncertain notice in the service provider safe harbor provisions of the DMCA and lack of notice in the governmental seizure of Internet domain names—are legislative failures to appreciate the necessity of notice in the realms of copyright liability and procedural due process. The third failure—naked notice in "pirate site" cases involving injunctions against nonparty online service providers—is a judicial failure to appreciate the insufficiency of notice to satisfy procedural due process requirements.

The DMCA's uncertain notice framework has created a litigious and risky environment for online service providers, who are unable to determine with reasonable certainty when their safe-harbor obligation to remove content is triggered. Lack of notice to domain name registrants prior to the government's seizure of their domain names violates the First and Fifth Amendments and, in some cases, causes harm without the possibility of redress for throngs of innocent third parties. Naked notice for nonparty online service providers who are impermissibly named in TROs and preliminary injunctions in "pirate site" cases violates procedural due process and offends the principles of equity that injunctive relief should further. Each of these failures can be corrected, however, in the concrete ways this article identifies.

not merely what the decree has forbidden, because it may have gone too far, but what it has power to forbid, an act of a party."); *see also supra* notes 253-54 and accompanying text.

[337] *See* Menell & Meurer, *supra* note 1.