UNCERTAINTY AS ENFORCEMENT MECHANISM: THE NEW EXPANSION OF SECONDARY COPYRIGHT LIABILITY TO INTERNET PLATFORMS

John Blevins†

This Article examines the role that legal uncertainty plays as a copyright enforcement mechanism against Internet platforms. In recent years, Internet platforms have faced a new wave of copyright enforcement actions arising from their users' activity. These actions include both civil secondary liability claims and public enforcement actions such as domain name seizures and criminal prosecution. In these enforcement actions, content owners understandably prefer broad secondary liability standards, but these standards remain subject to statutory and doctrinal constraints such as the DMCA safe harbor. Copyright owners, accordingly, are attempting to increase the breadth and expense of secondary copyright liability for Internet platforms by institutionalizing uncertainty within legal doctrine. From this perspective, prevailing in enforcement actions is less important than obtaining statutory and doctrinal constructions that create uncertain standards that raise the potential costs of enforcement proceedings upon Internet platforms. Below, I describe and critique this attempted expansion, and then propose measures to strengthen and clarify Internet platforms' defenses. In doing so, I reject proposals that liability in this context should be determined primarily through tort principles.

TABLE OF CONTENTS

INTRODUCTION 1823

I. THE BENEFITS OF UNCERTAINTY FOR COPYRIGHT OWNERS 1826

A. *The Legal Efforts Against Internet Platforms* 1827

B. *The Benefits of Uncertainty* 1829

1. The Benefits for Private Litigation 1829

† Associate Professor of Law, Loyola University New Orleans College of Law. I would like to thank Eric Goldman, James Grimmelmann, Stacey Lantagne, and Elizabeth Townsend-Gard for being willing to review drafts. I also thank participants of the faculty workshop at Loyola University New Orleans.

2. The Benefits for Public Enforcement 1833
II. INSTITUTIONALIZING UNCERTAINTY IN PRIVATE LITIGATION 1834
A. *Section 512 Safe Harbor—Blurring the Bright Lines* 1834
1. "Red Flag" Knowledge 1837
2. Adequate Notice 1840
3. Service Providers and Protected Services 1842
4. Reasonable Removal Policy 1844
5. Right to Control and Financial Benefit 1845
B. *The Decline of the* Sony *Defense* 1848
C. *Other Efforts to Increase Uncertainty* 1850
1. The Rise of Inducement Liability 1850
2. Expanding Direct Infringement 1853
3. Suing Investors 1855
III. INSTITUTIONALIZING UNCERTAINTY IN PUBLIC ENFORCEMENT ACTIONS 1856
A. *Domain Name Seizures* 1856
1. Technical and Legal Overview 1856
2. Uncertainty Through New Legislation 1858
3. Uncertainty Through New Statutory Interpretations 1860
B. *SOPA and PIPA* 1864
C. *Criminal Prosecution* 1867
IV. NORMATIVE ANALYSIS OF EXPANDED UNCERTAINTY 1870
A. *Policy Tradeoffs of Secondary Liability* 1871
B. *Secondary Liability and Internet Platforms* 1872
V. HOW TO BETTER PROTECT INTERNET PLATFORMS 1875
A. *The Importance of Clear Rules* 1876
B. *Increasing Certainty in Private Enforcement Actions* 1877
1. Improving the DMCA Safe Harbor 1878
2. Improving the *Sony* Defense 1882
C. *Increasing Certainty in Public Enforcement Actions* 1884
1. Reforming Domain Name Seizures 1884
2. Reforming Criminal Prosecutions 1886
3. Procedural Protections 1886
CONCLUSION 1887

INTRODUCTION

In 2011, a video-sharing site called Veoh won a big victory in the Ninth Circuit.[1] Funded by prominent investors such as Time Warner and former Disney CEO Michael Eisner, Veoh became one of the most popular video-sharing sites on the Internet.[2] Major record labels ultimately sued Veoh for secondary copyright liability, but Veoh prevailed at both the district court[3] and in the Ninth Circuit.[4] In modern copyright litigation, however, winning isn't everything. By the time the Ninth Circuit released its opinion, Veoh had gone bankrupt, citing excessive litigation costs.[5]

In 2012, the federal government arrested and indicted the operators of Megaupload, a cyberlocker site that provides "cloud" storage for its users' files.[6] The Megaupload indictment has been criticized as an extension of criminal liability to activity traditionally governed by civil secondary liability doctrines.[7] Regardless of its merits, the indictment prompted other cloud storage companies to alter their business practices shortly after the arrests.[8]

---

1 UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1026 (9th Cir. 2011), *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL 1092793 (9th Cir. Mar. 14, 2013). Since the original writing of this Article, the Ninth Circuit withdrew and replaced the original opinion. However, the superseding opinion does not substantively alter the points of law to which I cite, and therefore, I have retained all references to the Ninth Circuit's original opinion.

2 Jefferson Graham, *Veoh Aims to Be One-Stop Shop for Net TV Viewers*, USA TODAY, Feb. 27, 2008, at 8B (noting that Veoh has "quietly become the top independent U.S. video site on the Internet"); Press Release, Veoh Networks, Inc., Time Warner, Michael Eisner and Spark Capital Join Shelter Capital to Complete $12.5 Million Strategic Series B Investment in Veoh Networks (Apr. 18, 2006), *available at* http://www.veoh.com/corporate/pressroom/article/04_18_2006.

3 UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1100–01 (C.D. Cal. 2009), *aff'd sub nom.* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL 1092793 (9th Cir. Mar. 14, 2013).

4 *Shelter Capital Partners*, 667 F.3d at 1026.

5 *See* Mike Freeman, *Business Briefing*: *Web Video Company Veoh Plans Bankruptcy Filing*, SAN DIEGO UNION-TRIBUNE, Feb. 13, 2010, at C1; Michael Masnick, *Apparently Veoh Isn't Dead Enough for Universal Music*, TECHDIRT (Jan. 30, 2012), http://www.techdirt.com/articles/20120126/02350517545/apparently-veoh-isnt-dead-enough-universal-music-asks-rehearing-its-bogus-copyright-lawsuit.shtml; Corynne McSherry, *Ninth Circuit Puts Lump of Coal in UMG's Stocking*, ELEC. FRONTIER FOUND. (Dec. 20, 2011), https://www.eff.org/deeplinks/2011/12/ninth-circuit-puts-lump-coal-umgs-stocking-affirms-dmca-safe-harbors-veoh ("The cost of defending the case effectively drove Veoh out of business . . . . "); *see also infra* Part I.B.1.

6 Ben Sisario, *U.S. Charges Popular Site with Piracy*, N.Y. TIMES, Jan. 20, 2012, at B1.

7 *See infra* Part III.C.

8 *See* Phillip S. Corwin, *MegaBust's MegaQuestions Cloud the Net's Future*, CIRCLEID (Feb. 13, 2012), http://www.circleid.com/posts/megabusts_megaquestions_cloud_the_nets_future (describing reaction of other cyberlocker sites).

These two enforcement proceedings share common themes. In both, the Internet platforms were targeted because of the infringing actions of their users. In addition, in both cases, the parties enforcing copyrights succeeded in altering behavior without (or at least prior to) prevailing in the case. The Veoh litigation helped bankrupt the company even though federal courts ultimately ruled that the site was legal.[9] Similarly, the Megaupload indictment altered the behavior of other cyberlockers almost immediately. The lesson is that copyright enforcement against Internet platforms can often succeed merely by *increasing the potential costs of enforcement proceedings*.

In this Article, I explore the role that uncertainty plays as a copyright enforcement mechanism against Internet platforms. Specifically, I argue that uncertainty is the means by which copyright owners are attempting to increase the costs of enforcement proceedings for Internet platforms. Such costs can be increased either by expanding the breadth of secondary copyright liability (and thus making damages or penalties more likely) or by making the standards less clear (and thus more expensive to determine and litigate). Legal uncertainty, I argue, achieves both goals simultaneously.

In the abstract, though, uncertain standards are not inherently broader than clear rules.[10] One could imagine bright-line rules that establish expansive secondary liability. Copyright owners, however, operate within statutory and doctrinal constraints that limit platforms' liability for their users' actions. Increasing legal uncertainty thus provides a way to expand liability in the face of these constraints. Once established, it not only provides copyright enforcers with greater leverage, it creates incentives for Internet platforms to become co-enforcers of third-party copyrights. In short, uncertainty "outsources" enforcement costs to Internet platforms.

From this perspective, the recent wave of private and public enforcement proceedings against Internet platforms can be understood as efforts to expand and institutionalize legal uncertainty within secondary liability doctrines.[11] In the private litigation context, the key dispute is between rules that limit and clarify secondary liability, and standards that expand and blur its boundaries. I examine these disputes by focusing on the potential *defenses* Internet platforms have to secondary liability claims—particularly the DMCA safe harbor and *Sony* defenses.[12] In these cases, Internet platforms prefer statutory (or

9 *See infra* Part I.B.1.

10 One could imagine, for instance, a bright-line rule establishing extremely broad secondary liability for Internet platforms.

11 Technically, and as I explain in Part III, criminal secondary liability arguably does not exist. But because platforms face enforcement proceedings because of their users' activities, I use the word broadly to encompass both civil and criminal liability.

12 *See infra* Part II.A–B.

doctrinal) interpretations that create clear bright-line rules with low administrative costs. Copyright owners, by contrast, prefer statutory interpretations that impose vague fact-intensive standards. If adopted, these standards would not only increase the doctrine's breadth, they would also make it more difficult to halt litigation through early dispositive motions prior to discovery.

In the public context, I argue that the government is using uncertainty to expand secondary liability through new legislation and expansive interpretations of existing statutes. I examine these efforts in the context of domain name seizures, the controversial SOPA and PIPA bills, and criminal prosecutions.[13] In all of these contexts, the government is pursuing doctrines and interpretations that would blur and expand the boundaries of its enforcement authority through the use of vague and ambiguous text and interpretations.[14] This expansion, in turn, provides the government with greater leverage to pursue and threaten public enforcement proceedings.

Broader secondary liability, however, is not necessarily bad policy. In many instances, secondary liability provides an efficient and fair means of enforcing copyrights.[15] I argue, however, that Internet platforms possess unique characteristics and benefits that make broad secondary liability normatively problematic. In contrast to more traditional defendants, liability for Internet platforms imposes significant negative externalities by jeopardizing a vast range of legal, innovative, and expressive content.[16] Given the spillovers associated with Internet platforms, adopting bright-line rules that narrow and clarify secondary liability is a justifiable subsidy that outweighs the associated costs of infringement.[17]

My Article's primary contribution is to unite these seemingly distinct enforcement actions under the conceptual frame of uncertainty. This framing yields several descriptive and normative benefits. Descriptively, I illustrate that the key disputes in diverse enforcement actions can be understood as efforts to institutionalize—or to resist—legal uncertainty. Of course, several recent Articles have described the potential harms of uncertainty within secondary copyright liability

---

13 *See infra* Part III.

14 Vagueness and ambiguity have distinct meanings in the literature. "Vague" concepts are partially determinate and partially indeterminate, while "ambiguous" concepts have more than one meaning. *See* John T. Valauri, *Confused Notions and Constitutional Theory*, 12 N. KY. L. REV. 567, 570 (1985) ("A vague concept has a fringe of uncertainty around a core of settled meaning; an ambiguous concept has more than one focus of meaning."). In this Article, I generally use the term "uncertainty" to cover both concepts because they both lead to an *expansion* of secondary copyright liability in the face of statutory constraints that would otherwise protect Internet platforms.

15 *See infra* Part IV.A.

16 *See infra* Part IV.B.

17 *See infra* Parts IV.B, V.A.

doctrine (and copyright law more generally).[18] I expand upon these critiques, however, by illustrating how uncertainty specifically manifests in various enforcement actions against Internet platforms. My framing therefore helps rationalize recent trends in case law across several contexts, and better illustrates the practical implications of both the cases' holdings and the parties' respective arguments.

Normatively, my framing helps justify secondary liability standards for Internet platforms that are both narrow and clear. I argue that the unique social, economic, and technological features of Internet platforms justify bright-line rules that narrow the doctrine's scope and limit litigation costs.[19] One alternative normative approach in the literature is to use tort-like principles to determine the proper scope of platforms' liability.[20] This approach, however, underestimates the practical harms that Internet platforms face when the doctrine remains subject to more vague negligence-like standards.

Part I summarizes the private and public enforcement actions that Internet platforms currently face, and explains why uncertainty benefits copyright enforcers in these proceedings. Part II describes how uncertainty is being institutionalized within civil secondary liability doctrine, while Part III does the same for public enforcement doctrines. Part IV assesses the normative benefits of secondary liability generally, and argues that they are not present in proceedings against Internet platforms. Part V proposes measures to strengthen and clarify platforms' defenses through clear rules, and justifies these choices.

I. THE BENEFITS OF UNCERTAINTY FOR COPYRIGHT OWNERS

This Part provides an overview of the recent copyright enforcement actions against Internet platforms. I begin by describing

---

18 *See, e.g.*, Michael A. Carrier, *Copyright and Innovation: The Untold Story*, 2012 WIS. L. REV. 891, 944–45 (2012); David Fagundes, *Crystals in the Public Domain*, 50 B.C. L. REV. 139, 142–46 (2009); James Gibson, *Risk Aversion and Rights Accretion in Intellectual Property Law*, 116 YALE L.J. 882, 887–95 (2007); Lital Helman, *Pull Too Hard and the Rope May Break: On the Secondary Liability of Technology Providers for Copyright Infringement*, 19 TEX. INTELL. PROP. L.J. 111, 112–14 (2010); Lital Helman & Gideon Parchomovsky, *The Best Available Technology Standard*, 111 COLUM. L. REV. 1194, 1205–12 (2011); Steven J. Horowitz, *Copyright's Asymmetric Uncertainty*, 79 U. CHI. L. REV. 331, 332–35 (2012); Gideon Parchomovsky & Kevin A. Goldman, *Fair Use Harbors*, 93 VA. L. REV. 1483, 1491–1502 (2007); *see also* Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Appellees and Affirmance at 9–12, UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011) (No. 09-56777), 2010 WL 3706522, at *9–12 [hereinafter EFF Amicus Brief].

19 *See infra* Part IV.B.

20 *See, e.g.*, Helman & Parchomovsky, *supra* note 18, at 1196–98, 1216–17 & n.124 (proposing "best available technology standard"); Peter S. Menell & David Nimmer, *Legal Realism in Action: Indirect Copyright Liability's Continuing Tort Framework and* Sony*'s de Facto Demise*, 55 UCLA L. REV. 143, 149 (2007) (supporting the "traditional tort framework").

these platforms and summarizing the private and public enforcement actions they face. I then explain why uncertain legal doctrine benefits copyright enforcers in these proceedings.

A. *The Legal Efforts Against Internet Platforms*

Copyright enforcers target Internet platforms under the theory that they facilitate infringement by others.[21] The most common targets are platforms that support "user generated content" (UGC), which is content supplied independently by third-party users.[22] Examples of UGC platforms include many of the Internet's most popular sites: Facebook, Twitter, Wikipedia, YouTube, Pinterest, Tumblr, eBay, Amazon, Yelp!, Dropbox, Megaupload, Instagram, Wordpress, and Typepad to name a few.[23] Other common targets are "information location" sites such as search engines that help users locate—and link to—third-party content.[24] For brevity, I refer to both types of sites as "platforms."

Copyright enforcement actions tend to target certain categories of these platform services over others. The first targeted category is "cyberlocker" services, which provide online cloud storage for digital files of the user's choosing.[25] Once users upload their files, they can access them from other devices or share them publicly. Popular cyberlockers include Dropbox, iCloud, Mediafire, the Amazon and Google cloud storage services, and the infamous Megaupload. Other cyberlockers such as Grooveshark, Soundcloud, MP3Tunes, and Google Play focus on storing music files.[26] These platforms also include video-

---

21 Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345, 1346–47 (2004).

22 Steven Hetcher, *User-Generated Content and the Future of Copyright: Part One-Investiture of Ownership*, 10 VAND. J. ENT. & TECH. L. 863, 870–73 (2008) (defining UGC content).

23 Edward Lee, *Warming Up to User-Generated Content*, 2008 U. ILL. L. REV. 1459, 1460 (2008).

24 Hannibal Travis, *Opting Out of the Internet in the United States and the European Union: Copyright, Safe Harbors, and International Law*, 84 NOTRE DAME L. REV. 331, 349 (2008).

25 Examples of private litigation against cyberlockers include: *Perfect 10, Inc. v. Megaupload Ltd.*, No. 11-CV-0191, 2011 WL 3203117 (S.D. Cal. July 27, 2011); *Disney Enters., Inc. v. Hotfile Corp.*, 798 F. Supp. 2d 1303 (S.D. Fla. 2011); Complaint, Capitol Records, LLC v. ReDigi Inc., No. 12-CV-0095 (S.D.N.Y. Jan. 6, 2012), 2013 WL 1286134 [hereinafter *ReDigi* Complaint]; Complaint, UMG Recordings, Inc. v. Escape Media Grp. Inc., No. 11-CIV-8407 (S.D.N.Y. Nov. 18, 2011) [hereinafter Grooveshark Complaint]. Examples of public enforcement actions include: *Arista Records LLC v. Usenet.com, Inc.*, 608 F. Supp. 2d 409 (S.D.N.Y. 2009) (targeting Usenet provider); Indictment of Megaupload Operators, United States v. Dotcom, No. 1:12CR3 (E.D. Va. Jan. 5, 2012) [hereinafter *MegaUpload* Indictment].

26 For a recent overview of music lockers, see Brandon J. Trout, *Infringers or Innovators? Examining Copyright Liability for Cloud-Based Music Locker Services*, 14 VAND. J. ENT. & TECH. L. 729, 730–33 (2012).

sharing and photo-sharing sites that allow users to upload, store, and share their files.[27] The most popular video-sharing platform is YouTube, but the category also includes sites such as Veoh, Vimeo, Facebook, and Funnyordie. Photo-sharing sites include sites like Instagram, Pinterest, and Photobucket.

A second category of targeted platform services is "aggregator" sites that provide links to third-party infringing content.[28] These sites can include general search engines and online markets such as Amazon and eBay. They can also include sites that specialize in certain types of content, such as links to streams of sports videos.[29] Other aggregator sites allow users to search for, and link to, files stored within specific cyberlockers. These aggregation sites are generally independent from the cyberlockers, though sometimes the two coordinate.[30]

A third category is peer-to-peer file sharing services, which have featured prominently in copyright litigation for over a decade.[31] These companies provide software (and, in some instances, services) that allows users to locate and download files on individuals' computers in the absence of centralized architecture.[32] While my Article focuses on more modern UGC platforms such as cyberlockers, enforcement efforts continue against peer-to-peer file-sharing services such as Limewire and related aggregation sites such as Isohunt and Torrent-Finder.[33]

The various Internet platforms described above currently face both private and public copyright enforcement proceedings. By private

---

27 Examples of private litigation against these sites include: *Viacom Int'l, Inc., v. YouTube*, Inc., 676 F.3d 19 (2d Cir. 2012); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022 (9th Cir. 2011) (Veoh), *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL 1092793 (9th Cir. Mar. 14, 2013); *Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724 (S.D.N.Y. 2012) (Photobucket).

28 Aggregators have recently faced a wave of public enforcement actions such as domain name seizures and criminal prosecution. These actions include the seizure of Rojadirecta's domain name, and the prosecution of the operator of TVShack.com. *See infra* Part III.A, C. Private litigation against aggregators is not new, but has targeted sites like Google, Amazon, and eBay. *See, e.g.*, Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146 (9th Cir. 2007); Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090 (W.D. Wash. 2004); Hendrickson v. Amazon.com, Inc., 298 F. Supp. 2d 914 (C.D. Cal. 2003); Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

29 Rojadirecta linked to sporting event streams. *See infra* Part III.A.

30 The Megaupload indictment alleges that the company conspired with third-party aggregators. *Megaupload* Indictment, *supra* note 25, ¶¶ 11–14.

31 The three leading cases regarding peer-to-peer networks are *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005); *In re Aimster Copyright Litigation*, 334 F.3d 643 (7th Cir. 2003); and *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

32 Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 717–22 (2003) (discussing the elements of, and purity in, peer design).

33 Examples of private litigation include *Arista Records LLC v. Lime Group. LLC*, 784 F. Supp. 2d 398 (S.D.N.Y. 2011); and *Columbia Pictures Industries, Inc. v. Fung*, No. 06-CV-5578, 2009 WL 6355911 (C.D. Cal. Dec. 21, 2009). The federal government recently seized the domain name of Torrent-Finder, a "search engine for users of BitTorrent." Ben Sisario, *Piracy Fight Shuts Down Music Blogs*, N.Y. TIMES, Dec. 14, 2010, at B1.

enforcement, I mean civil litigation by rights holders, particularly the music and film industry. Plaintiffs in these cases generally allege direct and secondary liability claims.[34] The substance of their claims is that platforms should be liable for facilitating the infringement of others.[35] Public enforcement actions, by contrast, refer to domain name seizures and criminal prosecutions by the federal government. In these actions, the government generally alleges that the platform is committing criminal copyright infringement or is "facilitating" it.[36]

B. *The Benefits of Uncertainty*

This Section explains copyright owners' motives for preferring uncertain legal standards in enforcement proceedings against Internet platforms. In short, uncertainty increases the potential costs of enforcement proceedings in at least two ways. First, uncertainty includes vague and ambiguous standards that are more expensive to define and litigate. Second, uncertainty expands the breadth of secondary liability, thus making it more likely that a platform will face damages or penalties. These increased costs are especially harmful on Internet platforms, who often lack the resources to survive expensive litigation and whose activities (enabling third-party content) make them inherently susceptible to massive damages.

1. The Benefits for Private Litigation

In general, legal standards are more costly to enforce than bright-line rules in private litigation.[37] Legal standards can be especially expensive if they raise fact-intensive questions that require extensive discovery (document review, depositions, motions) and trials. Although higher litigation costs affect both parties, they disproportionately harm parties with fewer resources because each marginal dollar spent on

---

34 *See, e.g.*, Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1140 (N.D. Cal. 2008).

35 Lemley & Reese, *supra* note 21, at 1346–47.

36 *See, e.g.*, Affidavit in Support of Application for Seizure Warrant at 45, United States v. Rojadirecta.com, 2011 WL 320195 (S.D.N.Y. Jan 31, 2011) (No. 11-MAG-262) [hereinafter *Rojadirecta* Affidavit] (alleging Rojadirecta "commit[ed] and facilitate[d] criminal copyright infringement").

37 The general view is that rules are costlier to create but cheaper to enforce, while standards are cheaper to create but more expensive to enforce. Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557, 562–63 (1992); Russell B. Korobkin, *Behavioral Analysis and Legal Form: Rules vs. Standards Revisited*, 79 OR. L. REV. 23, 31–32, 56 (2000).

litigation effectively costs smaller parties more.[38] Further, the party with fewer resources has less ability to bear the risk of losing.[39]

The reality of contemporary copyright litigation against Internet platforms is that it often pits the film and music industries against startups that have comparatively less money and less secure sources of revenue.[40] For many Internet companies, the litigation itself can be fatal even if they are complying fully with copyright law. For these reasons, content industries can often "win" simply by filing litigation so long as the litigation is expensive.[41] The plaintiffs do not necessarily need to prevail on the merits—in many cases, they merely need to survive dispositive motions that would limit discovery or would halt the litigation altogether. Uncertain legal standards therefore help these copyright owners to the extent they generate additional fact-intensive questions that require extensive discovery and trials. As Helman and Parchomovsky observe, major copyright owners can use "ambiguous doctrines to threaten legal action against defendants who [lack] financial wherewithal to engage in lengthy and expensive legal battles."[42]

The bankruptcy of the startup Veoh illustrates this dynamic. Veoh was launched in 2005 as a video-sharing service.[43] Within a year of its launch, Veoh had attracted millions of dollars from well-known investors like Time Warner and former Disney executive Michael Eisner, who also served on its board.[44] By 2008, Veoh had signed distribution agreements with major broadcast networks, and was attracting millions of visitors per month, making it one of the most popular video sites on the Internet.[45] Veoh's ambitions also evolved as

---

38 Lisa Bernstein, *Social Norms and Default Rules Analysis*, 3 S. CAL. INTERDISC. L.J. 59, 78 n.67 (1993) ("The ability to threaten to impose high litigation costs will improve the bargaining position of the party with superior resources . . . .").

39 Fagundes, *supra* note 18, at 162–64.

40 For instance, Universal Music is suing Veoh and Grooveshark. UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011), *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL 1092793 (9th Cir. Mar. 14, 2013); Grooveshark Complaint, *supra* note 25, ¶¶ 3–4. Capitol Records is suing ReDigi. *ReDigi* Complaint, *supra* note 25, ¶¶ 5–6. Several music labels are collectively suing MP3Tunes and Limewire. Capitol Records, Inc. v. MP3Tunes, LLC, 821 F. Supp. 2d 627 (S.D.N.Y. 2011); Arista Records LLC v. Lime Grp. LLC, 715 F. Supp. 2d 481 (S.D.N.Y. 2010). Various movie studios are suing Isohunt and other related sites. Columbia Pictures Indus., Inc. v. Fung, No. CV 06-5578, 2009 WL 6355911, at *1 n.1 (C.D. Cal. Dec. 21, 2009). And while YouTube is not lacking for resources, it was sued by Viacom. Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010), *aff'd in part, vacated in part*, 676 F.3d 19 (2d Cir. 2012).

41 Helman & Parchomovsky, *supra* note 18, at 1208. ("[V]ague legal doctrines give rise to strike suits.").

42 *Id.* (citing Veoh as an example).

43 Graham, *supra* note 2. Veoh also had a peer-to-peer client application. *Id.*

44 Laura M. Holson, *Eisner Makes Hairpin Turn in His Career*, N.Y. TIMES, Apr. 17, 2006, at C11.

45 *See* Andy Fixmer & Leon Lazaroff, *Web Firms to Distribute CBS Shows on Internet*, WASH. POST, Apr. 13, 2007, at D03; Mike Freeman, *[San Diego's] Veoh Promoting TNT Series;*

the company sought to "democratize[] broadcasting" by becoming the world's first virtual cable network.[46]

Veoh, however, also attracted copyright litigation. In 2007, Universal Music Group (UMG), the country's largest record label, sued Veoh and Veoh's *investors*.[47] In December 2011, the Ninth Circuit confirmed what all previous lower courts had confirmed—that Veoh was legal and had complied with § 512's safe harbor.[48] The decision, however, came too late. Veoh filed for bankruptcy in 2010 citing its excessive litigation costs.[49] Even though Veoh did not violate copyright laws, the copyright litigation itself was enough to help bankrupt it.[50] Indeed, Veoh's general counsel argued that UMG filed "motion after motion" trying to bankrupt the company.[51] The founder of Veoh, Dmitry Shapiro, later added:

> [T]he lawsuit dramatically impacted our ability to operate the company. The financial drain of millions of dollars going to litigation took away our power to compete, countless hours of executive's time was spent in dealing [with] litigation, and employee morale was deeply impacted with a constant threat of shutdown. . . . To make sure that our money supply was cut off, in an unprecedented move, UMG sued not only the company, but our investors . . . personally.[52]

Shapiro is of course a non-neutral actor, and Veoh's finances were impacted by the recession and the rise of new competitors like Hulu.[53] The litigation, however, undeniably impacted the company's finances at a critical point just as it was poised to succeed. Like many startups, Veoh's survival depended on the ability to obtain private investment,

---

Web Video Startup Hopes to Stand Apart, SAN DIEGO UNION-TRIBUNE, July 13, 2006, at C-1; Peter Lauria, *Veoh's Way with Moguls*, N.Y. POST, Sept. 13, 2007, at 40; Brad Stone, *The Boat Is About to Rock (Again) in Internet Video*, N.Y. TIMES, July 15, 2007, at BU3.

46 Dan Fost, *Tech Chronicles*, S.F. CHRON., Nov. 11, 2006, at C1; *Veoh Sees New Service as "Virtual Cable,"* BOS. GLOBE, Feb. 13, 2007, at E4.

47 For the investor suit, see UMG Recordings, Inc. v. Veoh Networks Inc., No. CV 07-5744, 2009 WL 334022 (C.D. Cal. Feb. 2, 2009).

48 UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1026 (9th Cir. 2011), *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL 1092793 (9th Cir. Mar. 14, 2013); UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1100–01 (C.D. Cal 2009), *aff'd sub nom.* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL 1092793 (9th Cir. Mar. 14, 2013).

49 *See* Freeman, *supra* note 4.

50 Masnick, *supra* note 5; Janko Roettgers, *Appeals Court Reaffirms DMCA Defense in Veoh Court Victory*, GIGAOM (Dec. 20, 2011), http://www.gigaom.com/video/veoh-universal-appeal-decision.

51 Peter Lauria, *Veoh Wins Ruling over UMG*, N.Y. POST, Sept. 15, 2009, at 33.

52 Masnick, *supra* note 5.

53 Mike Freeman, *Veoh Networks Changes CEOs, Eliminates 25 Jobs*, SAN DIEGO UNION-TRIBUNE, Apr. 3, 2009, at C-1; Greg Sandoval, *Veoh Wins Copyright Case*, CNET NEWS (Sept. 14, 2009), http://news.cnet.com/8301-1023_3-10352183-93.html.

which can be sensitive to new developments like litigation—particularly when the litigation is directed at the investors themselves.[54]

The Viacom-YouTube litigation provides another illustration of this dynamic. In 2007, Viacom sued YouTube for one *billion* dollars.[55] Like Veoh, YouTube has been largely successful at both the district[56] and appellate[57] court levels, though its legal costs are estimated to be over $100 million thus far.[58] Unlike Veoh, YouTube survived the litigation because Google—its owner—could absorb the legal bills. Without Google, YouTube would have likely been sued out of existence. As Jack Balkin observed, "YouTube in 2005 [before the Google purchase] could not have survived such a lawsuit by Viacom."[59] Most UGC companies, however, lack access to such resources when faced with copyright litigation that poses an existential threat.

The costs of uncertain standards are compounded by the potential costs of liability. As a general matter, copyright violations give rise to a notoriously high and uncertain range of monetary damages.[60] Internet platforms, however, are particularly susceptible to high damages given that their business model depends on attracting as many users as possible. If popular platforms are found liable, statutory damages could run as high as $150,000 per work infringed.[61] Given the volume of content on Internet platforms, some have called statutory damages in this context "effectively infinite."[62]

The more general principle is that Internet platforms are particularly vulnerable to expensive copyright litigation. As legal standards become more uncertain and thus more expensive, private copyright litigation becomes progressively more threatening. Collectively, these risks create incentives for platforms to assume copyright enforcement costs by altering business practices or by adopting monitoring and filtering measures. Indeed, as I illustrate in Part II, the content industry is quite explicit about seeking legal

54 Carrier, *supra* note 18, at 914–15 ("Venture capital is crucial to startups . . . .").

55 Joe Nocera, *Awaiting a Compromise on YouTube*, N.Y. TIMES, Mar. 17, 2007, at C1.

56 Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010), *aff'd in part, vacated in part*, 676 F.3d 19 (2d Cir. 2012).

57 Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012).

58 YouTube won an almost complete victory in the district court. While the Second Circuit decision is generally considered a win for YouTube, I argue the opinion was more mixed. *See infra* Part II.A. On Google's legal fees, see Liz Shannon Miller, *Google's Viacom Suit Legal Fees: $100 Million*, GIGAOM (July 15, 2010), http://gigaom.com/video/googles-viacom-suit-legal-fees-100-million.

59 Jack Balkin, *The Real Issues in* Viacom v. YouTube, BALKINIZATION (June 25, 2010), http://balkin.blogspot.com/2010/06/real-issues-in-viacom-v-youtube.html.

60 *See, e.g.*, Alan E. Garfield, *Calibrating Copyright Statutory Damages to Promote Speech*, 38 FLA. ST. U. L. REV. 1, 6–7 (2010); Gibson, *supra* note 18, at 887 ("[T]he penalties for copyright infringement are severe").

61 17 U.S.C. § 504(c)(2) (2012).

62 Carrier, *supra* note 18, at 941.

standards that would effectively require Internet platforms to affirmatively police their own sites for copyright infringement.[63]

2. The Benefits for Public Enforcement

An important distinction between private and public enforcement actions is that the latter involves more severe penalties. Criminal liability is different in kind from civil liability in terms of both punishment and stigma.[64] And while domain name seizures are not the same as going to jail, they are an extreme remedy that can threaten the site's existence.[65] Because the potential costs of public enforcement actions can be significant, rational risk-averse actors will be very motivated to avoid them.

Critically, these public enforcement actions can serve the government's interests even when they do not ultimately succeed. For instance, the indictment of Megaupload has already changed cyberlockers' behavior even if the court ultimately dismisses the indictment. Following the indictment and arrest, several cyberlockers announced that they would modify or even discontinue several of their primary business practices.[66] Some sites disabled sharing altogether, while others vowed to terminate any subscriber that a content owner *suspects* is infringing.[67] The threat of jail apparently has a way of getting one's attention.

Similarly, the government's recent seizure of the domain name dajaz1.com—a popular hip-hop blog—also served the government's interests even though it proved a mistake. The government initially alleged that the site posted links to songs that had not yet been released.[68] As it turned out, artists and record labels had leaked the pre-

---

63 *See, e.g.*, Io Grp., Inc. v. Veoh Networks, Inc. 586 F. Supp. 2d 1132, 1154 (N.D. Cal. 2008) ("[Plaintiff's] not-so-subtle suggestion is that, if Veoh cannot prevent infringement from ever occurring, then it should not be allowed to exist."); *infra* Part II.5.

64 Dan Markel, *How Should Punitive Damages Work?*, 157 U. PA. L. REV. 1383, 1429 (2009) ("[A] civil sanction . . . is qualitatively different from criminal penalties because such damages entail no resulting conviction [and] less of a stigma.").

65 Ben Sisario, *Hip-Hop Copyright Case Had Little Explanation*, N.Y. TIMES, May 7, 2012, at B4.

66 Corwin, *supra* note 8; Michael Masnick, *Hollywood Continues to Kill Innovation, Simply by Hinting at Criminal Prosecution of Cyberlockers*, TECHDIRT (Apr. 4, 2012), http://www.techdirt.com/blog/innovation/articles/20120403/18090818360/hollywood-continues-to-kill-innovation-simply-hinting-criminal-prosecution-cyberlockers.html.

67 Timothy B. Lee, *Rapidshare Struggles to Placate Big Content with Anti-Piracy Plan*, ARS TECHNICA (Apr. 19, 2012), http://arstechnica.com/tech-policy/2012/04/rapidshare-struggles-to-placate-hollywood-with-anti-piracy-plan.html.

68 Application and Affidavit for Seizure Warrant at 56, United States v. Seizure Warrant, No. 10-2822M (C.D. Cal. Nov. 17, 2010) [hereinafter *Dajaz1* Seizure Warrant], *available at* https://www.eff.org/node/70613.

release songs to the blog for promotional reasons, and the government ultimately returned the domain name a year later—implicitly admitting its mistake. Even though Dajaz1 committed no copyright violation, the site was ultimately forced offline for a year.[69] As a result, other platforms now recognize that their own domain names could disappear without notice.

The larger point is that the mere possibility of public enforcement can increase costs on Internet platforms. Legal uncertainty magnifies these costs by effectively expanding the scope of the government's public enforcement authority. In short, as uncertainty increases, public enforcement becomes more plausible. This dynamic not only increases the government's leverage in demanding changes by platforms, it also creates incentives for platforms to alter behavior and to assume the enforcement costs of other parties' copyrights. For Internet startups in particular, these increased costs and risks make it harder to secure investment and to attract employees and users.

II. INSTITUTIONALIZING UNCERTAINTY IN PRIVATE LITIGATION

This Part argues that the legal disputes in private litigation can be understood as efforts to institutionalize—or to limit—uncertain legal standards with the secondary liability doctrines most relevant to Internet platforms. These doctrines include the § 512 safe harbor, the *Sony* doctrine, and other common law secondary liability standards. As I illustrate, this dispute manifests a conflict between rules and standards. Internet platforms prefer bright-line rules that narrow and clarify secondary liability, while copyright owners prefer vaguer standards that expand it.

A. *Section 512 Safe Harbor—Blurring the Bright Lines*

When Internet platforms are sued for copyright infringement, the first line of defense is the statutory safe harbor in § 512 of the Digital Millennium Copyright Act (DMCA).[70] Enacted in 1998, § 512 was a compromise between major content owners and technology companies.[71] Content owners feared that the Internet would enable an unprecedented wave of infringement, while technology companies

---

69 Sisario, *supra* note 65; Declan McCullagh, *DHS Abruptly Abandons Copyright Seizure of Hip-Hop Blog*, CNET NEWS (Dec. 8, 2011), http://news.cnet.com/8301-31921_3-57339569-281/dhs-abruptly-abandons-copyright-seizure-of-hip-hop-blog.

70 17 U.S.C. § 512 (2012).

71 For the most comprehensive account of the legislative process that led to the DMCA, see JESSICA LITMAN, DIGITAL COPYRIGHT 122–45 (2001).

feared being sued for providing general-purpose services such as data transmission and storage.[72] Private parties eventually hammered out a compromise, and Congress incorporated it into the DMCA.[73]

Section 512 is a complex statute, but the basic idea is simple. Defendants can invoke § 512 as an affirmative defense to infringement if they satisfy numerous statutory requirements. Qualifying defendants enjoy immunity from all monetary damages and most injunctive remedies as well.[74] A central dispute in these cases, therefore, is whether defendants who invoke § 512 comply with the various statutory prerequisites.[75]

Section 512 includes numerous formal requirements, but they can be grouped into general categories. The first is the threshold requirement that the party is a "service provider," which is defined broadly as "a provider of online services or network access, or the operator of facilities therefor."[76] The alleged infringement must also arise from protected services expressly listed in the statute. These include transmission services (§ 512(a)), caching (§ 512(b)), storage of information "at the direction" of users (§ 512(c)), and information location services (§ 512(d)). UGC platforms potentially qualify under § 512(c), while aggregation sites potentially fall under § 512(d).[77] Both sections, however, are substantively similar.[78]

Assuming a party is a service provider under § 512(c) or § 512(d), it must also comply with a miscellaneous set of provisions that (among

---

72 Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1098 (W.D. Wash. 2004); Neil Weinstock Netanel, *Locating Copyright Within the First Amendment Skein*, 54 STAN. L. REV. 1, 86 n.286 (2001); Elizabeth G. Thornburg, *Going Private: Technology, Due Process, and Internet Dispute Resolution*, 34 U.C. DAVIS L. REV. 151, 170 (2000).

73 The safe harbor provision was part of the Online Copyright Infringement Liability Limitation Act (OCILLA), which was codified as Title II of the DMCA. Pub. L. No. 105-304, § 201, 112 Stat. 2860, 2877 (1998); *see also* Menell & Nimmer, *supra* note 20, at 166. Regarding the traditional role of private parties drafting copyright legislation, see LITMAN, *supra* note 71, at 22–32.

74 Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 636 (S.D.N.Y. 2011); *Corbis*, 351 F. Supp. 2d at 1098 (noting that § 512 "protect[s] eligible service providers from all monetary and most equitable relief").

75 *See, e.g.*, *MP3tunes*, 821 F. Supp. 2d at 636 ("This case turns in large part on whether MP3tunes is eligible for protection under the safe harbors."); Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1141 (N.D. Cal. 2008) (considering DMCA eligibility prior to liability).

76 The statute creates two categories of service providers, though only the second category—defined by 17 U.S.C. § 512(k)(1)(B)—is relevant for our purposes. Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 26–27 (2d Cir. 2012); *In re* Aimster Copyright Litig., 252 F. Supp. 2d 634, 657 (N.D. Ill. 2002) ("The DMCA defines 'service provider' in two different ways, depending upon which safe harbor is at issue.").

77 17 U.S.C. § 512(a)–(d) (2012); *see also* Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J.L. & ARTS 233, 235–37 (2009).

78 Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J.L. & TECH. 253, 267 (2006) ("Section 512(d) offered nearly identical conditional protections to those available to OSPs under § 512(c).").

other things) ensure the provider is acting in good faith. These provisions include the "notice and takedown" regime, which requires platforms to remove content upon receiving a valid notice from a copyright owner.[79] Some of the commonly litigated "good faith" prerequisites include the following: 1) the defendant must not have "actual" or "apparent" knowledge of the infringing activity;[80] 2) the defendant must not enjoy a direct financial benefit from infringing activity that it has the right and ability to control;[81] 3) the defendant must have established adequate "notice and takedown" procedures and complied with them;[82] and 4) the defendant must have instituted and implemented adequate policies to remove repeat infringers.[83]

Section 512 also imposes several requirements upon the party seeking removal of the content. The most important is that the "notice" of infringing material must comply with various formal requirements.[84] If the notice is defective (e.g., too broad, lacking in detail), it cannot create the "knowledge" of infringement that would trigger takedown obligations.[85] Section 512 further protects technology companies by explicitly stating that they have no affirmative duty to monitor their sites for infringement.[86]

Section 512 thus imposes multiple and complex requirements on both parties in modern copyright litigation, though most of them fall on Internet platforms seeking to invoke the safe harbor. One implication of this complexity is that the plaintiffs need only prevail on *one* issue—one contested statutory provision—to deprive defendants of the safe harbor entirely. Defendants, by contrast, must prevail on every single issue.[87] And because § 512 imposes so many prerequisites, it creates incentives to litigate multiple statutory provisions.[88]

---

79 Ke Steven Wan, *Internet Service Providers' Vicarious Liability Versus Regulation of Copyright Infringement in China*, 2011 U. ILL. J.L. TECH. & POL'Y 375, 378–79 (2011).

80 17 U.S.C. § 512(c)(1)(A), (d)(1).

81 *Id.* § 512(c)(1)(B), (d)(2).

82 *Id.* § 512(c)(2).

83 *Id.* § 512(i)(1)(A).

84 *Id.* § 512(c)(3)(A), (d)(3).

85 *Id.* § 512(c)(3)(B)(i). In some instances, however, a partially compliant notice can create knowledge unless the service provider makes an effort to obtain a fully compliant one. *Id.* § 512(c)(3)(B)(ii).

86 *Id.* § 512(m)(1) (providing DMCA immunity not be conditioned on "a service provider monitoring its service or affirmatively seeking facts indicating infringing activity").

87 Eric Goldman, Viacom v. YouTube *Ruling Is a Bummer for Google and the UGC Community*, ARS TECHNICA (Apr. 6, 2012), http://arstechnica.com/tech-policy/2012/04/second-circuit-ruling-in-viacom-v-youtube-is-a-bummer-for-google-and-the-ugc-community.

88 Eric Goldman has critiqued the DMCA's complexity on these grounds. *See* Eric Goldman, *Photobucket Qualifies for the 512(c) Safe Harbor (Again)*—Wolk v. Kodak, TECH. & MKTG. BLOG (Jan. 22, 2012), http://blog.ericgoldman.org/archives/2012/01/wolk_v_kodak.htm; Eric Goldman, *supra* note 87.

In the Sections below, I examine the most contested statutory provisions of § 512. In each Section, I argue that the disputes surrounding these provisions can be understood as an interpretative fight between bright-line rules and standards. Internet platforms prefer bright-line interpretations that narrow liability and allow them to dispose of litigation at an early stage. Content owners, by contrast, prefer interpretations that incorporate uncertain legal standards that require fact-intensive discovery and broaden the doctrine.

Viewing these disputes through this lens yields several benefits. First, it helps clarify trends in the § 512 case law, and provides a better descriptive account of the case's holdings. Second, it illustrates content owners' efforts to institutionalize doctrinal uncertainty as an enforcement strategy. The key insight is that—for content owners—favorable statutory construction is more important than actual results. Content owners do not need to win § 512 cases—they only need to establish that the statutory provisions are fact-intensive standards that cannot be resolved by early dispositive motions. And because § 512 includes so many statutory requirements, the plaintiffs need only establish uncertainty *in one provision* to effectively neutralize the safe harbor. In short, a bad result with a good interpretation can be better than a good result with a bad interpretation. Further, increasing the vagueness of the doctrine—at least in this context—generally expands the breadth of the doctrine too. Thus, increasing uncertainty not only raises the costs of litigation, it also threatens to expose a broader range of platforms' conduct to high statutory damages.

1. "Red Flag" Knowledge

Section 512's safe harbor is unavailable if service providers have "actual" or "apparent" knowledge of infringing activity and fail to remove it.[89] These two levels of knowledge are distinct under the statute.[90] Actual knowledge is a purely subjective standard, while apparent knowledge—also called "red flag" knowledge—incorporates subjective and objective standards.[91] Red flag knowledge is created by awareness of "facts or circumstances from which infringing activity is apparent."[92] As the Second Circuit has explained, the service provider

---

89 17 U.S.C. § 512(c)(1)(A), (d)(1).

90 Clause (A)(i) prohibits "actual knowledge," while clause (A)(ii) prohibits "apparent knowledge." *Id.* § 512(c)(1)(A), (d)(1).

91 S. REP. NO. 105-190, at 44 (1998) [hereinafter Senate DMCA Report] ("The 'red flag' test has both a subjective and an objective element.").

92 17 U.S.C. § 512(c)(1)(A)(ii), (d)(1)(B).

must be "subjectively aware of facts that would have made the specific infringement 'objectively' obvious to a reasonable person."[93]

Understandably, copyright owners and Internet platforms disagree on how to construe these provisions. Internet platforms seek to narrow and clarify the range of facts that can create red flag knowledge. Accordingly, they prefer a clear rule that only *specific* knowledge of *specific* infringing activity triggers DMCA obligations.[94] In practice, this interpretation implies that knowledge is triggered only when copyright owners specifically identify infringement (generally by listing URLs) in a DMCA notice.[95] So long as platforms comply with these notices, they have certainty that red flag knowledge does not exist.

Content owners, by contrast, want to expand the range of facts that can create red flag knowledge. Accordingly, they argue that these provisions should be interpreted as broader standards. For instance, they contend that red flag knowledge requires only "generalized awareness" of infringement, as opposed to knowledge of specific instances of infringement.[96] They also argue that apparent knowledge encompasses "willful blindness" by platforms.[97] The key distinction, however, is these interpretations imply that facts *external* to the DMCA notice can give rise to knowledge.[98] Under this interpretation, the range of knowledge-triggering activity becomes far more uncertain and fact-specific. As a result, it would have the practical effect of shifting enforcement costs to platform owners. Because platforms will be more

---

93 Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2d Cir. 2012).

94 *See, e.g.*, Brief for Defendants-Appellees at 29–30, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012) (Nos. 10-3270-cv, 10-3342-cv), 2011 WL 1462232, at *29–31 (stating that DMCA requires "knowledge of specific and identifiable infringements of particular individual items"); Brief of Appellee Veoh Networks, Inc. at 34–35, UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011) (No. 09-56777), 2010 WL 3706519, at *34–35 [hereinafter *Veoh* Brief] (stating requirement of "knowledge of specific instances of actual infringement" (citations omitted)).

95 These arguments are documented in the next Section regarding adequate notice. *See infra* Part II.A.2.

96 *YouTube*, 676 F.3d at 31 ("[P]laintiffs urge the Court to hold that the red flag provision 'requires less specificity' than the actual knowledge provision."); UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1136–37 (9th Cir. 2011) (noting UMG's argument that "general knowledge" is sufficient), *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL 1092793 (9th Cir. Mar. 14, 2013); Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1108–09 (W.D. Wash. 2004); *see also* Brief of Amici Curiae Broadcast Music, Inc. et al. in Support of Appellants and Reversal at 22–23, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012) (No. 10-3270), 2010 WL 5167434, at *22–23 [hereinafter BMI *YouTube* Amicus Brief] ("The DMCA . . . leaves the 'facts and circumstances' constituting 'knowledge or awareness' to be decided on a case by case basis.").

97 *See, e.g.*, Brief for Motion Picture Association of America and Independent Film & Television Alliance as Amici Curiae Supporting Appellants at 22–25, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012) (No. 10-3270), 2011 WL 4541965, at *22–25 [hereinafter MPAA *YouTube* Amicus Brief] (contending the specific knowledge standard "encourages willful blindness").

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

uncertain about when knowledge exists, they will be more likely to monitor their sites aggressively and remove material liberally.[99]

The courts' approach to these questions has been muddled, but framing the dispute in terms of uncertainty helps clarify the case law. Over the past decade, the general trend has been toward a more narrow, rule-like interpretation of red flag knowledge. In some of the earlier cases involving peer-to-peer technologies, courts read the DMCA provisions as vague standards. For instance, in *Aimster*, the district court essentially equated the red flag provisions with the knowledge requirements of contributory liability (which are notoriously vague).[100]

As the decade progressed—and as defendants expanded beyond peer-to-peer companies—courts narrowed their interpretations. In the 2007 case *Perfect 10 v. Amazon.com*, the Ninth Circuit rejected the argument that apparent knowledge could arise from potential "red flags" such as the name of the URLs or from the hosting of password-breaking sites.[101] In the most recent cases, courts within the influential Ninth and Second Circuits have adopted even stronger rule-like interpretations that emphasize the specific knowledge requirement.[102] One common theme throughout these opinions is that a contrary interpretation would shift the burden of enforcement upon service providers in violation of the DMCA.[103]

---

99 *See, e.g.*, Brief for Amici Curiae Broadcast Music, Inc. and American Society of Composers, Authors and Publishers in Support of Appellants at 6–7, UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011) (No. 09-56777), 2010 WL 3706516, at *6 [hereinafter BMI Veoh Amicus Brief] (arguing representative list notice "triggers the service provider's duty to use its own monitoring technology to take reasonable action to investigate and stop infringing activity"); *see also* EFF Amicus Brief, *supra* note 18, at 20–21, 2010 WL 3706522, at *20–21.

100 *In re* Aimster Copyright Litig., 252 F. Supp. 2d 634, 661 (N.D. Ill. 2002) (holding constructive knowledge under common law contributory liability also nullifies a DMCA defense); *see also* Arista Records, Inc. v. Mp3Board, Inc., No. 00 CIV. 4660, 2002 WL 1997918, at *10 (S.D.N.Y. Aug. 29, 2002). On the vagueness of contributory liability, see *infra* note 170.

101 Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1113–15 (9th Cir. 2007).

102 Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 32 (2d Cir. 2012); UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1037–38 (9th Cir. 2011), *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL 1092793 (9th Cir. Mar. 14, 2013); Obodai v. Demand Media, Inc., No. 11-cv-2503, 2012 WL 2189740, at *6–7 (S.D.N.Y. June 13, 2012), *aff'd sub nom.* Obodai v. Cracked Entm't, No. 12-2450, 2013 WL 2321420 (2d Cir. May 29, 2013); Wolk v. Kodak Imaging Network, Inc., 840 F. Supp. 2d 724, 746–47 (S.D.N.Y. 2012); Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 643–45 (S.D.N.Y. 2011); Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 523–24 (S.D.N.Y. 2010), *aff'd in part, vacated in part*, 676 F.3d 19 (2d Cir. 2012); UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1110–12 (C.D. Cal. 2009), *aff'd sub nom.* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL 1092793 (9th Cir. Mar. 14, 2013); *see also* Lee, *supra* note 77, at 256.

103 *CCBill*, 488 F.3d at 1114–15 ("We do not place the burden of determining [legality] on a service provider."); *see also YouTube*, 718 F. Supp. 2d at 524 (quoting *CCBill*, 488 F.3d at 1114); *Shelter Capital Partners*, 667 F.3d at 1035–38 (same); Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1149 (N.D. Cal. 2008) (same).

The holdings, however, have not been uniformly consistent. Indeed, one benefit of my proposed framework is that it helps clarify distinctions between superficially similar holdings. One such distinction is the Ninth and Second Circuit's divergent approaches to red flag knowledge. On the surface, they seem similar in that both adopted rule-like interpretations that reject generalized awareness. The Second Circuit opinion, however, helps content owners more than some scholars initially thought.[104] First, the court held that "willful blindness" could establish apparent knowledge and remanded the case on that basis.[105] Second, the court also remanded because there was a material factual issue about whether specific knowledge existed—a decision based on several internal emails, largely limited to YouTube's first two years of existence.[106]

Together, these decisions undermine the court's other rule-like interpretations by introducing uncertain standards that future plaintiffs can exploit to increase the costs of litigation.[107] The willful blindness standard, for instance, requires factual information regarding the company's employees. It seems impossible, however, to address this issue without extensive factual discovery that includes depositions and examinations of internal emails—and maybe even trials. Similarly, the decision to remand on the basis of early internal emails helps future plaintiffs justify discovery of internal emails. And even though the Second Circuit attempted to limit its holding, the opinion injects just enough uncertainty to justify extended litigation, which is all content owners need to increase costs.

2. Adequate Notice

The DMCA requires that notices must comply with numerous formal requirements. Among other things, the DMCA requires copyright owners to provide an "identification of the copyrighted work" or—in the case of multiple works—a "representative list of such works at that site."[108] The "identification" must include "information reasonably sufficient" to allow the service provider "to locate the material."[109] Adequate notice creates both actual and apparent knowledge, which in turn triggers takedown obligations. Inadequate

104 David Post, Viacom v. YouTube *Decision—Not as Bad as All That*, VOLOKH CONSPIRACY (Apr. 6. 2012), http://www.volokh.com/2012/04/06/viacom-v-youtube-decision-not-as-bad-as-all-that.

105 *YouTube*, 676 F.3d at 34–35.

106 *Id.* at 32–34.

107 *See generally* Goldman, *supra* note 87.

108 17 U.S.C. § 512(c)(3)(A) (2012).

109 *Id.* § 512(c)(3)(A)(iii).

notices, by contrast, do not create such knowledge, and thus cannot—by themselves—trigger takedown obligations.[110]

The central dispute in this context turns on how specific a DMCA notice must be. Unsurprisingly, Internet platforms favor bright-line interpretations that narrow liability and lower their administrative costs. They argue that, in addition to complying fully with the formal requirements, DMCA notices must contain specific and easily identifiable infringing activity—generally in the form of a specific URL.[111] For platforms, the most important point is that a notice cannot create amorphous obligations to remove content not specifically listed in the notice.[112]

Amorphous standards, however, are exactly what copyright owners attempt to create, and they argue that the plain text supports this reading. For instance, the DMCA allows copyright owners to provide a "representative list" of infringing activity.[113] This provision, they argue, expressly contemplates infringing activity not specifically listed in a takedown notice.[114] The practical benefit of this interpretation is that it would allow a partial list of songs or artists to trigger an open-ended obligation to locate and remove other infringing activity.

Courts, however, have largely rejected copyright owners' arguments in recent cases. The consistent trend has been to interpret the notice provisions in a more rule-like fashion by limiting knowledge to the items specifically listed in the notice, and by being less forgiving of defective notices.[115] The shift began in 2003, when a district court ruled that notices must point to *current* infringing activity rather than potential future infringement.[116] The Ninth Circuit further narrowed

---

110 *Id.* § 512(c)(3)(B)(i). In some instances, a notice that *partially* complies with the DMCA can trigger obligations if the service provider does not make reasonable efforts to contact the notifying party and request a compliant notice. *Id.* § 512(c)(3)(B)(ii).

111 *See, e.g.*, Brief for Defendants-Appellees, *supra* note 94, at 57, 2011 WL 1357313, at *57 (arguing the DMCA does not require platforms "to respond to takedown notices by searching for *other* potentially infringing items beyond the specific materials that the [plaintiff] identified" (internal quotation marks omitted)).

112 *See, e.g.*, Memorandum in Support of Defendants' Motion for Summary Judgment at 19–20, Capitol Records, Inc. v. MP3tunes LLC, 821 F. Supp. 2d 627 (S.D.N.Y. 2011) (No. 07-Civ. 9931), 2010 WL 4632698, at *19–20.

113 17 U.S.C. § 512(c)(3)(A)(ii).

114 BMI Veoh Amicus Brief, *supra* note 99, at 9–11, 2010 WL 3706516, at *9–11 (noting narrow construction would "eviscerate the representative list provision"); *see also* Viacom Int'l Inc. v. YouTube, Inc., 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).

115 Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 30–32 (2d Cir. 2012); UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1036–38 (9th Cir. 2011), *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL 1092793 (9th Cir. Mar. 14, 2013); Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1111–13 (9th Cir. 2007); Wolk v. Kodak Imaging Network, Inc., 840 F. Supp. 2d 724, 746–47 (S.D.N.Y. 2012); Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 6432–43 (S.D.N.Y. 2011).

116 Hendrickson v. Amazon.com, Inc., 298 F. Supp. 2d 914, 917–18 (C.D. Cal. 2003).

this interpretation in 2007 by ruling that DMCA notices must comply with "all" provisions. Content owners cannot "cobble together adequate notice from separately defective notices."[117] One striking aspect of the court's decision is the strongly worded policy defense of holding notices to strict formal compliance. It noted that "[a]ccusations of alleged infringement have drastic consequences," including the removal of First Amendment-protected speech.[118] For this reason, complying with the formal requirements is very important.

More recent opinions have echoed these narrow rule-like interpretations. In *MP3tunes*, the district court held that a notice identifying "all songs" was defective.[119] In *UMG*, the Ninth Circuit held that merely identifying a list of artists was insufficient.[120] And in *YouTube*, the district court held that a notification listing a specific infringing clip creates no obligation to remove other versions of the clip at different locations.[121] Such a requirement, the court held, "would eviscerate the required specificity of notice," and would violate § 512(m), which expressly relieves defendants of the duty to affirmatively monitor their sites.[122] While recognizing that the DMCA allows representative lists, courts also note that the information must be "reasonably sufficient to permit the service provider to locate the material." This language, they conclude, implies a formal requirement of specificity.[123]

3. Service Providers and Protected Services

As explained above, the DMCA imposes threshold requirements on defendants invoking the safe harbor. The party must be a "service provider" under § 512(k)(1),[124] and the infringement must arise from a specified protected service.[125] The litigation relevant to this Article focuses on services protected by § 512(c) (data storage by users) and § 512(d) (information location). The precise language of § 512(c) shields

---

117 *CCBill*, 488 F.3d at 1111–13.

118 *Id.* at 1112.

119 *MP3Tunes*, 821 F. Supp. 2d at 642.

120 *Shelter Capital Partners*, 667 F.3d at 1039.

121 Viacom Int'l Inc. v. YouTube, Inc., 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).

122 *Id.*

123 *Id.*; UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1110 (C.D. Cal. 2009), *aff'd sub nom.* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL 1092793 (9th Cir. Mar. 14, 2013).

124 This Article focuses primarily on the second type of "service provider" under 17 U.S.C. § 512(k)(1)(B).

125 17 U.S.C. § 512(a)–(d) (2012).

platforms from liability for infringement "by reason of storage at the direction of a user."[126]

Courts have interpreted these requirements broadly and platforms generally satisfy them easily. For over a decade, courts have observed there is "uniform agreement that the definition [of 'service provider'] is broad"[127] and covers a "broad variety of Internet activities."[128] Courts have also adopted broad interpretations of the protected services listed in § 512(c)–(d).[129] In particular, courts have consistently affirmed that the DMCA protects not just storage, but other related features that are "attributable to" storage.[130] These broad interpretations have been so consistent that they have arguably evolved into a bright-line rule. Under this precedent, Internet platforms can be confident that their services will easily satisfy the DMCA's threshold requirements.

Despite this precedent, copyright owners continue to litigate these issues aggressively. In particular, they argue that "by reason of storage" should be interpreted more narrowly so that it protects only a subset of services that platforms provide.[131] The crux of their strategy is to identify additional services ancillary to storage that are not technically "storage."[132] In the Veoh litigations, content owners argued that various software functions associated with video uploads fall outside § 512(c)'s

---

126 *Id.* § 512(c)(1).

127 Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1175 (C.D. Cal. 2002) ("Section 512(k)(1)(B)'s definition has been interpreted broadly."); *see also In re* Aimster Copyright Litig., 252 F. Supp. 2d 634, 658 (N.D. Ill. 2002) ("[W]e have trouble imagining the existence of an online service that *would not* fall under the definitions . . . ."), *aff'd*, 334 F.3d 643 (7th Cir. 2003); Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082, 1088 (C.D. Cal. 2001).

128 Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1099–1100 (W.D. Wash. 2004).

129 Obodai v. Demand Media, Inc., No. 11-cv-2503, 2012 WL 2189740, at *7 (S.D.N.Y. June 13, 2012), *aff'd sub nom.* Obodai v. Cracked Entm't, No. 12-2450, 2013 WL 2321420 (2d Cir. May 29, 2013); Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 639–40 (S.D.N.Y. 2011); Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 526–27 (S.D.N.Y. 2010), *aff'd in part, vacated in part*, 676 F.3d 19 (2d Cir. 2012); UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1106–16 (C.D. Cal. 2009), *aff'd sub nom.* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL 1092793 (9th Cir. Mar. 14, 2013); Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1145–48 (N.D. Cal. 2008); Costar Grp. v. Loopnet, 164 F. Supp. 2d 688, 701 (D. Md. 2001), *aff'd*, 373 F.3d 544 (4th Cir. 2004).

130 UMG Recordings, Inc. v. Veoh Networks, Inc., 620 F. Supp. 2d 1081, 1089 (C.D. Cal. 2008); *see also* Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 38–40 (2d Cir. 2012); UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1031–35 (9th Cir. 2011), *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL 1092793 (9th Cir. Mar. 14, 2013).

131 *See, e.g.*, Memorandum of Law in Support of Viacom's Motion for Partial Summary Judgment at 61, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d. Cir. 2012) (No. 10-3270), 2010 WL 1004561 ("Defendants fall outside the DMCA . . . [because] their infringement does not result from providing the *specified* core Internet functions covered by the defense.").

132 *See, e.g.*, Appellants' Brief at 11–12, 31–48, UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011) (No. 09-56777), 2010 WL 3706518, at *11–12, *31–48 [hereinafter *UMG* Brief].

protected services.[133] For instance, when users uploaded videos to Veoh, the platform automatically converted the files into different formats (such as Flash) to make it easier for users on diverse devices to access. Veoh also streamed the files to users. The plaintiffs argued that both the file conversion and the playback functions were not "storage," and thus fall outside of § 512(c)'s protections.[134] The plaintiffs in YouTube raised similar arguments.[135]

The logic of the plaintiffs' strategy is to convert a rule into a standard. They do not necessarily need to "win" these disputes at trial; they merely need to transform the *statutory construction* into a more standard-like inquiry that requires factual discovery regarding the platforms' various features. If plaintiffs can persuade courts that factual issues exist regarding any single ancillary software function, that holding can be used to extend litigation and obtain discovery in future cases. It also would significantly broaden secondary liability by narrowing a key feature of the safe harbor.

4. Reasonable Removal Policy

Section 512(i) requires service providers to "adopt" and "reasonably implement" a policy for terminating users who are repeat infringers in "appropriate circumstances."[136] These requirements are designed to ensure the good faith of parties invoking the safe harbor. Section 512(i)—which uses terms like "reasonably" and "appropriate"—is drafted in the language of standards. Indeed, in *Cybernet Ventures*, the district court complained that § 512(i) and its legislative history were "less than models of clarity."[137] And courts in the early DMCA cases often ruled for copyright owners by finding factual issues regarding platforms' removal policies.[138]

More recent cases, however, demonstrate a clear trend toward a rule-like interpretation of these provisions that narrows platform liability and lowers administrative costs. The Ninth Circuit's 2007 opinion in *CCBill* illustrates this interpretative shift. After noting that the statute does not define "reasonably implement," it announced a new *element-based* definition.[139] The court held that parties "implement"

133 *Shelter Capital Partners*, 667 F.3d at 1031–32; *Io*, 586 F. Supp. 2d at 1146–48.

134 *Shelter Capital Partners*, 667 F.3d at 1031–32; *Io*, 586 F. Supp. 2d at 1146–48.

135 *YouTube*, 676 F.3d at 38–39.

136 17 U.S.C. § 512(i)(1)(A) (2012).

137 Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1176 (C.D. Cal. 2002).

138 *Id.* at 1175–79; *see also In re* Aimster Copyright Litig., 252 F. Supp. 2d 634, 658–59 (N.D. Ill. 2002), *aff'd*, 334 F.3d 643 (7th Cir. 2003); Costar Grp. v. Loopnet, 164 F. Supp. 2d 688, 703–04 (D. Md. 2001), *aff'd*, 373 F.3d 544 (4th Cir. 2004).

139 Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1109–10 (9th Cir. 2007).

policies if they have "a working notification system, a procedure for dealing with [takedown notices], and if [they do] not actively prevent copyright owners from collecting information needed to issue such notifications."[140] It also clarified that "reasonableness" does not require service providers to "affirmatively police" its users.[141] Together, these definitions significantly clarify and formalize § 512(i)'s requirements. And later courts have relied on this clarification in ruling for platforms on this issue.[142]

5. Right to Control and Financial Benefit

One of the safe harbor's most important requirements is that a service provider must not receive a direct financial benefit from infringing activity that it has the "right and ability to control."[143] These two requirements—financial benefit and control—are worded identically to courts' traditional definition of vicarious liability (one of the three secondary liability doctrines in copyright law).[144] A key issue, then, is whether the DMCA requirements are coextensive with vicarious liability standards. If so, the DMCA—by its plain text—would never apply to vicarious liability claims.[145]

Copyright owners, unsurprisingly, argue that the two doctrines are coextensive.[146] Under accepted interpretative canons, when Congress uses terms that have "settled meaning under common law," then the court should infer that Congress intends that meaning unless "the statute otherwise dictates."[147] Because the DMCA's language did have settled meaning, courts should therefore infer the requirement is coextensive with vicarious liability. The implication is that § 512 directly incorporates the common law vicarious liability standards.

---

140 *Id.*

141 *Id.* at 1111.

142 Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 637–39 (S.D.N.Y. 2011) (applying *CCBill*, 488 F.3d 1102); Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1142–45 (N.D. Cal. 2008) (applying *CCBill*, 488 F.3d 1102).

143 17 U.S.C. § 512(c)(1)(B), (d)(2) (2012).

144 Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 262 (9th Cir. 1996) ("[O]ne may be vicariously liable if he has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities." (quoting Gershwin Publ'g v. Columbia Artist Mgmt., 443 F.2d 1159, 1162 (2d Cir. 1971))). *But see* Lee, *supra* note 77, at 240–42 (arguing the text differs from common law standard).

145 Rebecca Giblin, *A Bit Liable? A Guide to Navigating the U.S. Secondary Liability Patchwork*, 25 SANTA CLARA COMPUTER & HIGH TECH. L.J. 7, 44 (2009); Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101, 113–14 (2007).

146 *UMG* Brief, *supra* note 132, at 67–69, 2010 WL 3706518, at *67–69 (arguing that DMCA provisions "track the elements of vicarious liability under long-standing copyright principles"); BMI *YouTube* Amicus Brief, *supra* note 96, at 26, 2010 WL 5167434, at *26.

147 *See, e.g.*, Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1117–18 (9th Cir. 2007) (quoting Rossi v. Motion Picture Ass'n of Am. Inc., 391 F.3d 1000, 1003 (9th Cir. 2004)).

This interpretation not only prevents platforms from invoking the safe harbor for vicarious liability claims, it is also uniquely well suited to raise litigation costs. To understand why, we must briefly review vicarious liability's historical evolution. Originally, vicarious liability had a more narrow scope. With roots in agency law, it was an equitable doctrine designed to prevent employers (or principals) from enjoying the benefits of their infringing employees (or agents).[148] Through time, however, the doctrine expanded well beyond its agency law foundations.[149] In particular, the holdings from cases like *Fonovisa* and *Napster* define "financial benefit" and "control" so broadly that they plausibly apply to any Internet platform.[150] Thus, by incorporating the common law standard into § 512, copyright owners would benefit from vague and fact-intensive standards that are broad, difficult to resolve in dispositive motions, and categorically immune from DMCA defenses.

The Viacom-YouTube case provides a concrete example of how these broad standards can lead to expensive discovery. In pre-trial motions, Viacom filed a motion to compel high volumes of information from YouTube—including "undisputed trade secret[s]."[151] The court granted some requests, and denied others.[152] The key point, however, is that plaintiffs justified many of these requests by invoking vicarious liability standards. The information, they argued, was necessary to "show that defendants have an ability to *control* infringement."[153] The plaintiffs in the *Io* litigation raised similar arguments in discovery.[154]

In light of these costs, Internet platforms argue that the DMCA requirements are distinct from traditional vicarious liability standards. The text of the statute presents challenges for this argument, so they have relied on broader arguments premised on the statute's overall structure, purpose, and legislative history.[155] Specifically, they argue that copyright owners' interpretations would effectively nullify the safe

---

148 Craig A. Grossman, *The Evolutionary Drift of Vicarious Liability and Contributory Infringement: From Interstitial Gap Filler to Arbiter of the Content Wars*, 58 SMU L. REV. 357, 363, 406–08 (2005).

149 *Id.* at 370–71; Sverker K. Högberg, *The Search for Intent-Based Doctrines of Secondary Liability in Copyright Law*, 106 COLUM. L. REV. 909, 929–30 (2006); Lee, *supra* note 77, at 236–37; Lemley & Reese, *supra* note 21, at 1366–68.

150 Helman & Parchomovsky, *supra* note 18, at 1198–99 ("The scope of these doctrines is so broad that in principle indirect liability could attach to most active websites."); Högberg, *supra* note 149, at 929–33; Lemley & Reese, *supra* note 21, at 1367–68.

151 Viacom Int'l Inc. v. Youtube, Inc., 253 F.R.D. 256, 258 (S.D.N.Y. 2008) (granting in part Viacom's motion to compel production).

152 *Id.* at 265.

153 *Id.* at 262–63 (emphasis added).

154 Io Grp., Inc. v. Veoh Networks, Inc., No. C06-03926, 2007 WL 1113800, at *3–4 (N.D. Cal. Apr. 13, 2007).

155 *See, e.g.*, *Veoh* Brief, *supra* note 94, at 50–53 (arguing the UMG interpretation "negates the purpose of the DMCA").

harbor and impose affirmative monitoring costs upon them.[156] Indeed, copyright owners can be explicit about seeking interpretations that require affirmative monitoring. As the MPAA argued in *YouTube*, the "entire point of vicarious liability is to incentivize the party . . . to uncover and remedy infringing conduct" from which it benefits.[157]

Courts have been inconsistent on these questions, to put it mildly.[158] Despite the extensive confusion surrounding these provisions, viewing the opinions in terms of rules versus standards provides some clarity. First, this framing illustrates why some recent opinions—particularly the Ninth Circuit's in *UMG* and the district court's in *YouTube*—can be understood as efforts to inject bright-line rules into these statutory provisions. In both cases, the courts interpreted the DMCA language as being different from traditional vicarious liability standards. The key distinction, they held, was that the DMCA imposed a *knowledge* requirement.[159] At first glance, this construction seems strange given that common law vicarious liability does not require knowledge.

The construction, however, makes perfect sense when viewed as an attempt to reduce the uncertainty of these provisions. Recall that these courts narrowed and clarified "red flag knowledge" by requiring specific identifications of specific infringing activity. By holding that the DMCA's benefit/control provisions *also* incorporate knowledge, the courts effectively imported the specific knowledge requirement to these provisions as well. As the *UMG* court noted, "we hold that the 'right and ability to control' under § 512(c) requires control over *specific infringing activity the provider knows about*."[160] In effect, specific identification is now required not merely for red flag knowledge, but for the financial benefit and control standards too. In this way, this court transformed

---

156 Brief of Amici Curiae eBay, Inc. et al. in Support of Appellee at 18–25, UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011) (No. 09-56777), 2010 WL 3706523, at *18–25 (stating that a contrary interpretation "would defeat the purpose of the DMCA . . . [and creates] 'natural incentive[s]' to censor user-contributed content" (quoting Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082, 1093 (C.D. Cal. 2001)) (internal quotation marks omitted)).

157 MPAA *YouTube* Amicus Brief, *supra* note 97, at 6, 2011 WL 4541965, at *6.

158 For cases interpreting the DMCA similarly to the common law standard, see Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1117–18 (9th Cir. 2007); Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1150 (N.D. Cal. 2008). For cases interpreting the DMCA differently, see Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 36 (2d Cir. 2012); UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1043–45 (9th Cir. 2011), *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL 1092793 (9th Cir. Mar. 14, 2013).

159 *Shelter Capital Partners*, 667 F.3d at 1041–45 ("[W]e conclude that a service provider must be aware of specific infringing material to have the ability to control [it.]"); Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 527 (S.D.N.Y. 2010), *aff'd in part, vacated in part*, 676 F.3d 19 (2d Cir. 2012).

160 *Shelter Capital Partners*, 667 F.3d at 1043 (emphasis added).

the common law standard into a more narrow and formalistic rule that could support dispositive motions.

A similar logic applies to courts' analysis of whether the ability to remove material constitutes per se "control." The majority trend is that that control requires "something more" than simply the ability to remove content or terminate users.[161] It would be illogical if an activity contemplated by the safe harbor (i.e., removal of content) simultaneously precluded its use.[162] While this interpretation is not exactly a bright-line rule, it does formalize the requirements somewhat by preventing plaintiffs from pursuing litigation (and discovery) based purely on allegations that platforms "control" users because they could block them.

Finally, this framework also illustrates another harmful aspect of the Second Circuit's *YouTube* opinion for Internet platforms. The Second Circuit rejected the Ninth Circuit's knowledge requirement as a-textual.[163] The court did not, however, provide an alternative interpretation—it merely disagreed with both parties' interpretations and remanded.[164] The result is that the Second Circuit introduced significant doctrinal *uncertainty*, which is arguably more important than the ultimate result because it provides a justification for extensive discovery. For these reasons, Eric Goldman has predicted that plaintiffs will forum shop cases in the Second Circuit, where the doctrine is far more unsettled.[165]

B. *The Decline of the* Sony *Defense*

Assuming platforms are ineligible for the safe harbor, courts must still determine whether they meet the requirements for secondary liability. Courts currently recognize three categories of secondary liability—contributory liability, vicarious liability, and inducement liability.[166] The common law doctrines of contributory and vicarious liability have a long history,[167] and the Copyright Act of 1976 implicitly

---

161 *See, e.g.*, *YouTube*, 676 F.3d at 37; *Shelter Capital Partners*, 667 F.3d at 1043; Wolk v. Kodak Imaging Network, Inc., 840 F. Supp. 2d 724, 747–48 (S.D.N.Y. 2012); *Io*, 586 F. Supp. 2d at 1151; Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1109–10 (W.D. Wash. 2004).

162 *Io*, 586 F. Supp. 2d at 1151 ("[A] contrary holding would render the DMCA internally inconsistent . . . ."); *see also YouTube*, 676 F.3d at 36–38.

163 *YouTube*, 676 F.3d at 36.

164 *Id.* at 38.

165 Goldman, *supra* note 87 ("I expect future 512 cases will be brought in the Second Circuit, not the Ninth Circuit.").

166 Alfred C. Yen, *Third-Party Copyright Liability After* Grokster, 91 MINN. L. REV. 184, 193, 224 (2006).

167 Jane C. Ginsburg, *Separating the* Sony *Sheep from the* Grokster *Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs*, 50 ARIZ. L. REV. 577,

recognizes them even though it does not expressly define them.[168] Inducement liability is more recent, and was created by the Supreme Court in the 2005 *Grokster* case.[169]

These doctrines are vague, and courts have struggled to define them for decades. Indeed, the literature has documented the confusion surrounding secondary liability standards—particularly contributory and vicarious liability.[170] I will not duplicate this analysis, but instead observe that Internet platforms cannot escape litigating vague and fact-intensive standards if they are ineligible for the safe harbor. Accordingly, I focus here on a separate defense that could potentially halt litigation in its early stages: the *Sony* defense.

The basics of *Sony* are well known. In 1984, the Supreme Court saved the VCR from copyright litigation.[171] VCRs were dual use, general-purpose devices that could be used for both infringing and non-infringing uses. Some consumers used VCRs to infringe, while others did not. One issue in *Sony*, then, was whether VCR manufacturers could be secondarily liable for the infringement of their users.[172] The Supreme Court rejected this argument, holding that devices "capable of substantial noninfringing uses" cannot be liable for secondary infringement.[173]

The meaning of *Sony* is sharply contested, but the language of the original opinion is worded as a clear rule strongly protective of new general-purpose technologies. Indeed, the opinion states that devices need only be *capable* of substantial noninfringing use to avoid secondary liability.[174] The practical benefits of this interpretation for technology companies are clear. When faced with secondary liability claims, defendants can cite a few noninfringing uses and resolve the case in an early dispositive motion. As Justice Breyer would explain years later in *Grokster*, the original *Sony* rule "deliberately [made] it difficult for courts to find secondary liability where new technology is at issue."[175]

579–81 (2008); Menell & Nimmer, *supra* note 20, at 152–53.

168 Grossman, *supra* note 148, at 360–61; Lemley & Reese, *supra* note 21, at 1354; Menell & Nimmer, *supra* note 20, at 153; R. Anthony Reese, *The Relationship Between the ISP Safe Harbors and the Ordinary Rules of Copyright Liability*, 32 COLUM. J.L. & ARTS 427, 428 n.4 (2009).

169 Metro-Goldwyn-Mayer Studios v. Grokster, 545 U.S. 913 (2005); Dotan Oliar, *The Copyright-Innovation Tradeoff: Property Rules, Liability Rules, and Intentional Infliction of Harm*, 64 STAN. L. REV. 951, 1010 (2012).

170 Mark Bartholomew & Patrick F. McArdle, *Causing Infringement*, 64 VAND. L. REV. 675, 678–79 (2011); Giblin, *supra* note 145, at 48–49; Högberg, *supra* note 149, at 914; Yen, *supra* note 166, at 187–88.

171 Sony Corp. of Am. v. Universal City Studios, 464 U.S. 417, 420–21 (1984).

172 *Id.* at 436–42.

173 *Id.* at 442.

174 *Id.* ("[W]e need not explore *all* the different potential uses of the machine . . . . ").

175 Metro-Goldwyn-Mayer Studios v. Grokster, 545 U.S. 913, 957–58 (2005).

The *Sony* defense, however, has evolved from a bright-line rule into a more limited and uncertain standard. Accordingly, the defense has become less useful for Internet platforms. As Lemley and Reese have written, the *Napster* court reinterpreted *Sony* in a way that significantly limited its scope.[176] Specifically, the Ninth Circuit held that *Sony* is not a full defense, but merely a presumption against imputing knowledge based on distribution of a dual use device.[177] Another interpretation of *Napster* is that *Sony* potentially applies to dual-use products (such as the VCR), but not to *services* such as Napster's ongoing search functionality.[178] The Seventh Circuit narrowed *Sony* in a different way. In *Aimster*, it suggested that the *Sony* defense applies only if the *primary* uses of the device are non-infringing.[179] The Supreme Court further muddied the *Sony* defense in its 2005 *Grokster* opinion. The Court confirmed that evidence of intentional inducement could overcome a *Sony* defense. It declined, however, to quantify "significant" noninfringing use, and left "further consideration of the *Sony* rule for a day when that may be required."[180]

The result is that the *Sony* defense is now an uncertain standard of unknown value.[181] The original decision contemplated a bright-line rule that defeated all secondary liability claims. In some circuits, however, *Sony* arguably applies only to contributory liability, and not to vicarious and inducement liability claims.[182] For these reasons, the *Sony* defense provides little remedy against extended discovery. Thus, even if *Sony* helps platforms ultimately win, its uncertainty ensures that the win will come at a high cost.

C. *Other Efforts to Increase Uncertainty*

1. The Rise of Inducement Liability

Inducement liability is the third and most recent category of secondary copyright liability. Because of its recent origins, inducement liability has introduced significant uncertainty to secondary liability

176 Lemley & Reese, *supra* note 21, at 1356–57.

177 A&M Records v. Napster, 239 F.3d 1004, 1020 (9th Cir. 2001); Tim Wu, *The Copyright Paradox*, 2005 SUP. CT. REV. 229, 234 ("One reading of *Sony* takes the language 'merely capable' to create a presumption.").

178 Ginsburg, *supra* note 167, at 592 n.61; Helman, *supra* note 18, at 126; Julie Erin Land, *The Risks of Using Secondary Liability Legislation as a Means of Reducing Digital Copyright Infringement*, 15 DEPAUL-LCA J. ART & ENT. L. 167, 193–94 (2004).

179 *In re* Aimster Copyright Litig., 334 F.3d 643, 649–52 (7th Cir. 2003).

180 *Grokster*, 545 U.S. at 933–34.

181 Oliar, *supra* note 169, at 961 ("Doctrinally, the contours of *Sony*'s safe harbor remain vague.").

182 Högberg, *supra* note 149, at 927–28 & n.102.

claims in several different respects. Indeed, lower courts have split on whether inducement is an independent category of secondary liability, or a subset of contributory liability.[183] My framing, however, helps clarify some the precise disputes involved.

The *Grokster* opinion itself attempted to strike a balance between the interests of copyright owners and technology companies. The problem was peer-to-peer companies whose decentralized software was consciously designed to avoid contributory and vicarious liability.[184] These companies had strong arguments that they had no knowledge or control over users' activities because they merely distributed software (a *product* like the VCR) that users could use as they see fit. At the same time, however, peer-to-peer technologies facilitated massive infringement. The Court's challenge was to craft a holding that reached some of these services, but whose logic would not extend to other general-use technologies that facilitate infringement (such as computers or operating system software).[185]

Inducement liability was the Court's attempt to thread this needle. It held that a party distributing general-use technologies could be liable for "inducing" copyright. The Court's specific language is important—it held that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."[186] The compromise embedded in this holding is evident. On the one hand, copyright owners have a new theory of secondary liability. On the other, the Court imposes additional requirements designed to protect technologies—namely, a specific intent requirement that must be established by objective "affirmative steps." The hope, presumably, was that the definition would be broad enough to cover peer-to-peer technologies, but narrow enough to avoid ensnaring other technologies within secondary liability claims.

---

183 For examples of cases treating it explicitly as an independent category, see Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 28 n.5 (2d Cir. 2012); Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124, 150–51 (S.D.N.Y. 2009). For examples of cases treating it as a subset of contributory liability, see *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1170 (9th Cir. 2007); *Arista Records LLC v. Lime Grp. LLC*, 784 F. Supp. 2d 398, 424 n.23 (S.D.N.Y. 2011); and *Columbia Pictures Indus., Inc. v. Fung*, No. CV 06-5578, 2009 WL 6355911 (C.D. Cal. Dec. 21, 2009), *aff'd in part as modified*, 710 F.3d 1020 (9th Cir. 2013).

184 William Henslee, *Copyright Infringement Pushin': Google, Youtube, and Viacom Fight for Supremacy in the Neighborhood That May Be Controlled by the DMCA's Safe Harbor Provision*, 51 IDEA 607, 620 (2011); Alfred C. Yen, *Torts and the Construction of Inducement and Contributory Liability in* Amazon *and* Visa, 32 COLUM. J.L. & ARTS 513, 513–14 (2009) ("The *Grokster* Court adopted inducement because the traditional doctrines of contributory and vicarious liability did not express the full range of rationales supporting third party liability.").

185 Högberg, *supra* note 149, at 948–49.

186 Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 936–37 (2005).

When viewed through the lens of uncertainty, however, the *Grokster* opinion is less protective than it first appears. For Internet platforms, a doctrine that increases litigation costs is harmful even when platforms ultimately win. And while *Grokster* appears to be protective of most platforms on paper, the practical reality is it creates a new standard that could potentially justify intrusive discovery.[187] For instance, one area of uncertainty is the types of evidence that constitute "affirmative steps" of inducement. As *Grokster* itself illustrates, internal emails and memoranda can be important sources of such unlawful objectives.[188] Accordingly, it will often be difficult to prove specific intent without access to these internal communications in discovery. So although *Grokster* attempts to craft a narrow holding, its new standard creates uncertainty by potentially requiring expensive discovery and extended litigation. It is of course possible that the recent heightened pleading standards established by *Twombly*[189] and *Iqbal*[190] could remedy these concerns, but it is too soon to know if the cases will have a tangible effect on inducement cases.[191]

These potential effects raise the important question of whether the DMCA safe harbor applies to inducement claims.[192] The stakes of this question are high. If the DMCA applies, then inducement claims can be dismissed in early dispositive motions. In this respect, a broader interpretation of the DMCA's scope would limit the uncertainty that the *Grokster* standard introduces. If, however, the DMCA does *not* apply, then copyright owners can rely on inducement claims to obtain discovery that the DMCA safe harbor would otherwise prevent.

Courts have split on the question of whether the DMCA—which preceded *Grokster* by several years—applies to inducement claims. Some courts have held that inducement liability is inherently inconsistent with the DMCA safe harbor.[193] Because the DMCA only protects innocent parties, those who have a specific intent to infringe are necessarily excluded. More recent opinions, however, have applied the DMCA to inducement claims. In the Veoh litigation, both the district court and the Ninth Circuit upheld the DMCA defense to inducement liability claims.[194] The Second Circuit in *YouTube* also seemed to adopt this

187 Wu, *supra* note 177, at 247–48.

188 *Grokster*, 545 U.S. at 938–40.

189 Bell Atl. Corp. v. Twombly, 550 U.S. 544 (2007).

190 Ashcroft v. Iqbal, 556 U.S. 662 (2009).

191 *See generally* Arthur R. Miller, *From* Conley *to* Twombly *to* Iqbal*: A Double Play on the Federal Rules of Civil Procedure*, 60 DUKE L.J. 1, 9–10 (2010).

192 *See generally* Reese, *supra* note 168.

193 Columbia Pictures Indus., Inc. v. Fung, No. CV 06-5578, 2009 WL 6355911, at *18 (C.D. Cal. 2009) ("[I]nducement liability and the Digital Millennium Copyright Act safe harbors are inherently contradictory."), *aff'd in part as modified*, 710 F.3d 1020 (9th Cir. 2013).

194 UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1030–31 (9th Cir. 2011), *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL

position, stating that "a finding of safe harbor application necessarily protects a defendant from all affirmative claims for monetary relief."[195]

The *YouTube* opinion, however, may be less protective than it seems. In a separate part of the opinion, the court hinted that inducement of infringement "might also rise to the level of control" for purposes of the DMCA.[196] If courts adopt this approach, the *Grokster* standard could lead to extended discovery—not as an independent category—but as part of the DMCA's "right and ability to control" provisions. In any event, the intersection of the DMCA with inducement liability raises several unsettled questions.

2. Expanding Direct Infringement

If platforms are ineligible for the DMCA safe harbor, they can also be potentially liable for *direct* infringement.[197] One benefit of alleging direct infringement is that copyright owners can establish liability without meeting the various requirements of secondary liability standards. While broad, these standards do at least require establishing something more than direct infringement.[198] In recent litigation, copyright owners have tried to expand the set of activities that give rise to direct infringement. These efforts, I argue, can be understood as attempts to replace relatively bright-line rules with more vague standards.

One example is the effort to transform video embeds into infringing "displays."[199] As background, courts have consistently held that "merely linking" to third-party content cannot establish direct infringement.[200] In *Perfect 10 v. Amazon.com*, the Ninth Circuit

1092793 (9th Cir. Mar. 14, 2013); UMG Recordings, Inc. v. Veoh Networks, Inc., 620 F. Supp. 2d 1081, 1083 (C.D. Cal. 2008) (rejecting UMG's initial summary judgment motion).

195 Viacom Int'l, Inc., v. YouTube, Inc., 676 F.3d 19, 41 (2d Cir. 2012).

196 *Id.* at 38.

197 CoStar Grp., Inc. v. LoopNet, Inc., 373 F.3d 544, 555 (4th Cir. 2004) ("[T]he DMCA is irrelevant to determining what constitutes a prima facie case of copyright infringement.").

198 MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 941 (9th Cir. 2010). ("[S]econdary copyright infringement . . . requires the existence of direct copyright infringement." (citations omitted)).

199 *See* Flava Works, Inc. v. Gunter (*Flava Works II*), No. 10 C 6517, 2011 WL 3876910, at *3–4 (N.D. Ill. Sept. 1, 2011) (denying motion for reconsideration of Flava Works, Inc. v. Gunter (*Flava Works I*), No. 10 C 6517, 2011 WL 3205399 (N.D. Ill. July 27, 2011), *rev'd by* Flava Works, Inc. v. Gunter (*Flava Works III*), 689 F.3d 754 (7th Cir. 2012)).

200 Perfect 10 v. Google, Inc., 416 F. Supp. 2d 828, 838 n.9 (C.D. Cal. 2006) ("Google does not risk liability for direct infringement merely by linking to content hosted on and served by third-party websites."), *aff'd in part, rev'd in part sub nom.* Perfect 10 v. Amazon.com, Inc., 487 F.3d 701 (9th Cir. 2007); Field v. Google, Inc., 412 F. Supp. 2d 1106, 1115 (D. Nev. 2006) ("[A]utomated, non-volitional conduct by Google in response to a user's request does not constitute direct infringement under the Copyright Act."); Online Policy Grp. v. Diebold, Inc., 337 F. Supp. 2d 1195, 1202 (N.D. Cal. 2004) ("[H]yperlinking per se does not constitute direct

extended this rule to Google's "inline links," which displayed images hosted on third-party servers.[201] Critically, Google did not host these images on its own servers, but merely directed a user's browser to the third-party server that stored them. The court explained that this process "does not constitute direct infringement of the copyright owner's display rights."[202] In short, it was just another form of linking.

The court's reasoning is known as the "server test," which holds that parties that do not "store and serve" the content do not directly infringe.[203] The server test is an example of a clear rule. If a platform does not store infringing content on its servers, it does not directly infringe. One implication of the server test is that embedding third-party video (e.g., embedding YouTube clips on blogs) does not directly infringe. Video embeds are simply another form of linking in that the embedded source code directs a browser to the server (such as YouTube's) that stores and transmits the video images.[204]

A federal district court, however, recently held that video embeds *can* give rise to direct infringement.[205] In this case, the defendant was a video bookmarking site called MyVidster, which allowed users to "flag" videos and share them with others. Critically, MyVidster did not host videos, but essentially linked to the videos (using embed codes) that were stored on other servers.[206] This holding, which contradicts virtually every known precedent, captured the attention of major industry representatives such as Google, Facebook, and the MPAA who filed amicus briefs on appeal. For our purposes, the most interesting aspect of the appeal was the interpretative dispute it created. Internet platforms argued that the bright-line "server test" rule should apply to video embeds.[207] The MPAA, by contrast, wanted to replace this rule with a broader standard that allows video embeds (and other links) to constitute direct infringement. It further argued that these issues must be "decided on its facts"—which can be understood as an attempt to institutionalize a more vague standard.[208] The Seventh Circuit ultimately

---

copyright infringement because there is no copying . . . . "); Arista Records, Inc. v. Mp3Board, Inc., No. 00 CIV. 4660, 2002 WL 1997918, at *3–4 (S.D.N.Y. Aug. 29, 2002); Ticketmaster Corp. v. Tickets.com, Inc., 54 U.S.P.Q.2d (BNA) 1344, 1345–46 (C.D. 2000) ("[H]yperlinking does not itself involve a violation of the Copyright Act . . . . ").

201 Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1160–61 (9th Cir. 2007).

202 *Id.*

203 *Id.* at 1159.

204 Brief of Amici Curiae Google Inc. and Facebook, Inc. in Support of Neither Party at 10–15, *Flava Works III*, 689 F.3d 754 (7th Cir. 2012) (No. 11-3190), 2011 WL 7962183, at *10–15 [hereinafter Google *Flava Works* Amicus Brief].

205 *Flava Works I*, No. 10 C 6517, 2011 WL 3876910, at *3–4 (N.D. Ill. Sept. 1, 2011).

206 *Flava Works III*, 689 F.3d 754, 756 (7th Cir. 2012).

207 Google *Flava Works* Amicus Brief, *supra* note 204, at 3–4, 2011 WL 7962183, at *3–4.

208 Brief for Motion Picture Ass'n of America as Amicus Curiae Supporting Appellants at 7–13, 9 n.7, *Flava Works III*, 689 F.3d 754 (7th Cir. 2012) (No. 11-3190).

reversed the district court.[209] While the opinion provided little clarity, the court's primary rationale was that MyVidster users were not infringing copyright, even assuming they may have been "stealing" from copyright owners by viewing the videos without paying.[210] As the court explained, "[t]he facilitator of conduct that doesn't infringe copyright is not a contributory infringer."[211]

In sum, the ultimate result of the litigation is arguably less important than the copyright owners' attempt to transform a doctrine that both limits and clarifies platforms' secondary liability into a broader and more vague one.

3. Suing Investors

The claim against Veoh's investors in their personal capacity represents a different type of effort to increase legal uncertainty.[212] Generally speaking, an important principle of American corporate law is that "shareholders are not responsible for a company's liabilities and that their loss cannot exceed the amount they invest in the corporation."[213] The Veoh investor suits—like the suits against Napster's investors[214]—can be understood as attempts to undermine these predictable rules in ways that expand secondary liability in uncertain ways.

Specifically, this type of litigation threatens to raise costs on all Internet platforms by causing investors to avoid platforms or to demand additional compensation for the risk. Indeed, one concern is that investors facing personal liability suits have significantly less protections than the Internet platforms themselves. Because individual investors are not "service providers," they cannot invoke the DMCA safe harbors.[215] These concerns are not abstract. Michael Carrier recently conducted a study of various executives in technology companies, and that the *Napster* decision created a chilling effect upon innovation and investment.[216] Further, he explained that secondary copyright liability might preclude venture capital firms from invoking indemnification provisions because liability requires "knowing" conduct.[217]

---

209 *Flava Works III*, 689 F.3d at 762–63.

210 *Id.* at 757–58.

211 *Id.* at 758.

212 UMG Recordings, Inc. v. Veoh Networks Inc., No. CV 07-5744, 2009 WL 334022 (C.D. Cal. Feb. 2, 2009).

213 Carrier, *supra* note 18, at 941.

214 *Id.* at 941–43.

215 *See supra* note 76.

216 Carrier, *supra* note 18, at 893–96.

217 *Id.* at 942–43.

Recognizing these policy concerns, both the district court and the Ninth Circuit in *UMG* dismissed the investor suits before full discovery.[218] The Ninth Circuit criticized the plaintiffs' "*novel* theory of secondary liability," which suggests the court viewed the suit as violating established norms.[219] Interestingly, both courts dismissed the claims by adopting clear holdings that would make it easier for future investors to halt litigation in early dispositive motions prior to discovery. For instance, the courts ruled that it would not presume that the board members appointed by the various investor-defendants acted "in concert" for purposes of secondary liability.[220] The Ninth Circuit cited this premise to dismiss all three claims.[221] The district court further found that general actions of board members do not rise to the level of "material contribution" or "direct financial benefit."[222] The benefit of these holdings for Internet platforms is that they establish administrable bright-line holdings that future investors could use in a motion to dismiss.

III. INSTITUTIONALIZING UNCERTAINTY IN PUBLIC ENFORCEMENT ACTIONS

This Part examines the efforts to institutionalize uncertainty within public enforcement proceedings. These efforts include enacting new legislation that both expands government authority and creates vague and ambiguous standards. They also include interpreting existing statutory text in novel ways that achieve similar ends. The Part focuses on three contexts: 1) domain name seizures; 2) the legislative efforts to pass SOPA and PIPA; and 3) criminal copyright prosecution.

A. *Domain Name Seizures*

1. Technical and Legal Overview

Domain names help users identify sites on the Internet.[223] All computers on the Internet are assigned an IP (Internet Protocol)

---

218 UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1045–47 (9th Cir. 2011), *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL 1092793 (9th Cir. Mar. 14, 2013); UMG Recordings, Inc. v. Veoh Networks Inc., No. CV 07-5744, 2009 WL 334022, at *1 (C.D. Cal. Feb. 2, 2009).

219 *Shelter Capital Partners*, 667 F.3d at 1047 (emphasis added); *see also id.* at 1046–47.

220 *Id.* at 1046–47; *Veoh Networks*, 2009 WL 334022, at *3.

221 *Shelter Capital Partners*, 667 F.3d at 1045–47.

222 *Veoh Networks*, 2009 WL 334022 at *3–6.

223 For general overview of the domain name process, see Jack Mellyn, *"Reach Out and*

address, which is a long string of numbers that computers use to locate other computers. These numbers, however, are impossible to remember, so sites generally obtain domain names that computers translate into numerical IP addresses. For instance, if you type in the domain name google.com, that domain name must be translated to an IP number in order for your computer to locate Google's servers. You do not necessarily need the domain name to reach Google—if you know the IP number, you can type it directly into the browser. But domain names are much easier to remember.

The Domain Name System (DNS) is the set of rules and protocols that allow computers to translate domain names into IP numbers. DNS works like a giant phone book.[224] When users type in google.com, the computer must "ask" the phone book what IP number corresponds to that domain name. DNS works because it is hierarchical and standardized.[225] Without standardization, computers using different "phone books" may not be able to locate certain sites, or may include erroneous "listings."

The key actors in the DNS hierarchy are domain name registries and registrars.[226] Registries are responsible for all domain names within a "top level domain" (TLD) such as .com or .org or .edu. Registrars, by contrast, are companies who assign and administer domain names within a TLD.[227] The translation process begins at the top of the hierarchy with the registries and eventually moves down to find the precise domain name. For instance, a computer seeking to translate "google.com" would begin with the .com TLD registry maintained by the registry (e.g., Verisign). The registry would then direct the computer to the registrar (e.g., GoDaddy) who administers that particular domain name registration. Eventually, the computer would find the "listing" that includes the IP number.[228]

Domain name seizures operate by changing the "phone book" listings at the very top of the DNS hierarchy. Assume that the government wanted to seize "pirate.com." The government could order

---

Touch Someone": The Growing Use of Domain Name Seizure as a Vehicle for the Extraterritorial Enforcement of U.S. Law, 42 GEO. J. INT'L L. 1241, 1246 (2011); Dennis S. Prahl & Eric Null, *The New Generic Top-Level Domain Program: A New Era of Risk for Trademark Owners and the Internet*, 101 TRADEMARK REP. 1757, 1761–62 (2011).

224 Jesse S. Bennett, *Caching in on the Google Books Library Project: A Novel Approach to the Fair Use Defense and the DMCA Caching Safe Harbors*, 35 FLA. ST. U. L. REV. 1003, 1016–17 (2008).

225 *Id.* at 1016–18.

226 Michael P. Allen, *In Rem Jurisdiction from* Pennoyer *to* Shaffer *to the Anticybersquatting Consumer Protection Act*, 11 GEO. MASON L. REV. 243, 248–50 (2002).

227 *Id.*

228 Mellyn, *supra* note 223, at 1245–46. This is of course a simplified version of the process; detailing the more technical aspects of the DNS process is not necessary for the purposes of this Article.

the registry operator for this domain (Verisign) to change the IP address associated with pirate.com. Instead of directing the user's computer toward the actual site, the "phone book" would redirect users to a different site—one that displays a message from the federal government indicating that the site has been seized.[229] The process is similar to calling your friend, only to find that the number is now connected to a government operator.

The government's statutory authority to seize domain names for copyright infringement is relatively new, and stems from the 2008 PRO-IP Act.[230] The statute itself, however, does not expressly reference domain names. Instead, § 2323(a) makes the following "property" subject to forfeiture: 1) any "article" whose "making or trafficking" violates various criminal copyright and trademark statutes; and 2) "any property used, or intended to be used, in any manner . . . to commit or *facilitate* the commission of" listed criminal offences.[231] The government's theory is that domain names are "property" that "facilitates" criminal copyright infringement. Indeed, many of the seized domain names direct users to sites that do traffic counterfeit goods, though the more problematic seizures have included music blogs (dajaz1.com) and directories of sports streaming sites (rojadirecta.com).[232]

2. Uncertainty Through New Legislation

The PRO-IP Act illustrates how Congress can expand the government's copyright enforcement authority by enacting vague and ambiguous text. When Congress enacted the law in 2008, no one anticipated that it authorized seizing domain names. Indeed, domain name seizures were not discussed in the legislative history, nor in the critiques of the bill in 2007 and 2008. For instance, the House committee report described increased authority to seize *tangible* physical items like servers "used to provide the [infringing or counterfeit] services."[233] Similarly, critics of PRO-IP expressed concern

---

229 Robert A. Heverly, *Breaking the Internet: International Efforts to Play the Middle Against the Ends—A Way Forward*, 42 GEO. J. INT'L L. 1083, 1106–07 (2011).

230 Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008, Pub. L. No. 110-403, 122 Stat. 4256 (codified in scattered sections of 15 U.S.C., 17 U.S.C., and 18 U.S.C.); *see also* Ann Chaitovitz et al., *Responding to Online Piracy: Mapping the Legal and Policy Boundaries*, 20 COMMLAW CONSPECTUS 1, 7–8 (2011).

231 18 U.S.C. § 2323(a)(1)(A)–(B) (2012). For convenience, I will refer to these provisions generically as "§ 2323(a)."

232 Timothy B. Lee, *Domain Seizure Oversight Lax and Broken*, ARS TECHNICA (Dec. 13, 2011), http://arstechnica.com/tech-policy/2011/12/expert-domain-seizure-oversight-too-lax-targets-out-of-luck.

233 H.R. REP. No. 110-617, at 41 (2008).

about overbroad seizures of servers, along with a damages provision that was ultimately removed.[234] There is simply no evidence that domain name seizures were ever contemplated as Congress debated the bill.

Domain name seizures, accordingly, were made possible not by explicit textual authority, but from vague text that the government subsequently interpreted in unexpected and expansive ways.[235] In short, the government's interpretations have transformed vague text into ambiguous text that potentially applies to entirely new and unforeseen set of actions.[236]

Interestingly, the bill's language became increasingly expansive as the bill progressed through Congress. Originally, the bill adopted a more narrow definition of "facilitating" that included strong protections for third-party services. The initial House bill (which passed in May 2008) provided that the government could only seize "facilitating" property if it was "owned or predominantly controlled by the violator" and if the government could "establish . . . a substantial connection between the property and the [violation]."[237] The accompanying committee report noted that violators' use of "commercially valuable digital communications or e-commerce services" would not constitute facilitation "absent extraordinary circumstances."[238] In short, the bill originally made "facilitating" difficult to establish.

Most of this language, however, had been removed when the bill moved to the Senate in July 2008. In this version, facilitators no longer had to "own or predominantly" control the property. Instead, the statute authorized forfeiture of property used "in any manner or part" to facilitate the offense. The statute did, however, continue to require a "substantial connection" between the property and the violation.[239] On September 26, 2008, Senator Leahy introduced an amended bill. This bill—which is the modern PRO-IP Act—no longer included the "substantial connection" language.[240]

---

234 *See, e.g.*, Nate Anderson, *House Committee Hears the Cons of the PRO-IP Act*, ARS TECHNICA (Dec. 13, 2007), http://arstechnica.com/tech-policy/2007/12/house-committee-hears-the-cons-of-the-pro-ip-act; Alex Curtis, *A Perfect Storm of Bad Copyright Legislation*, POLICY BLOG (Sept. 10, 2008), http://www.publicknowledge.org/node/1733 ("[T]he bill potentially opens up online services to having their servers seized even if they're not the ones who committed the infringement.").

235 Michael Masnick, *Why Operation in Our Sites Is Illegal and Needs to Be Fixed ASAP*, TECHDIRT (May 23, 2011), http://www.techdirt.com/articles/20110521/14304814372/why-operation-our-sites-is-illegal-needs-to-be-fixed-asap.shtml.

236 For the distinction between vagueness and ambiguity, see *supra* note 14.

237 H.R. REP. No. 110-617, at 5–8, 41 (2008).

238 *Id.* at 41.

239 S. 3325, 110th Cong. § 2 (2008) (as reported by S. Comm. on the Judiciary, July 24, 2008).

240 S. 3325, 110th Cong. § 2 (2008) (as passed by Senate, Sept. 26, 2008). It is possible—though unclear—that the "substantial connection" requirement duplicated the requirement of 18 U.S.C. § 983(c) and was unnecessary.

In sum, as the bill progressed through Congress, the government's authority became more uncertain and more expansive. These revisions removed the extensive protections for third parties that the original House report had emphasized in justifying the bill. As a result, the statute became a fertile source of novel enforcement actions such as domain name seizures. If the original language—particularly the provisions requiring violators to own or predominantly control the facilitating property—had remained in place, the government would have probably lacked authority for its more problematic seizures. In this respect, the history of PRO-IP provides guidance for the legislative debates surrounding SOPA and PIPA that I address later in the Article.[241]

3. Uncertainty Through New Statutory Interpretations

The government has also increased its enforcement authority through expansive interpretations of statutory text. In this Section, I illustrate this dynamic by examining the seizure of the domain names associated with the Spanish website Rojadirecta (rojadirecta.com and rojadirecta.org), and the legal proceedings that followed. The government ultimately withdrew its case against Rojadirecta following a year and a half of litigation (and thus before courts resolved the issues presented).[242] The arguments the government raised, however, illustrate the broader effort to institutionalize uncertainty and could easily be applied to a separate platform in the future.

Rojadirecta is an online forum for sports fans. The site provides discussion forums, and includes links to third-party content—generally streams of sporting events.[243] Rojadirecta organizes the links to sports streams into categories such as "Today on Internet TV," and "Download Last Full Matches."[244] Rojadirecta does not host these streams, but instead links to third party sites that do.[245] Some of these streams infringe copyrights, while others do not. Copyright owners challenged Rojadirecta in Spain, but Spanish courts had ruled that its operation was legal.[246]

---

241 *See infra* Part III.B.

242 Jennifer Martinez, *US Government Dismisses Piracy Case Against Rojadirecta Site*, THE HILL: HILLICON VALLEY (Aug. 29, 2012), http://thehill.com/blogs/hillicon-valley/technology/246529-us-government-dismisses-case-against-rojadirecta.

243 James Temple, *Don't Be Overzealous on Copyright*, S.F. CHRON., June 15, 2011, at D1.

244 *Rojadirecta* Affidavit, *supra* note 36, at 37–38.

245 Memorandum of Points and Authorities in Support of Puerto 80's Petition for Release of Seized Property and in Support of Request for Expedited Briefing and Hearing of the Same at 2–3, Puerto 80 Projects, S.L.U. v. United States, No. 1:11-03983 (S.D.N.Y. June 13, 2011).

246 Temple, *supra* note 243.

In February 2011, pursuant to a warrant, the Immigration and Customs Enforcement agency (ICE) seized Rojadirecta's domain names under § 2323(a), which authorizes forfeiture of property used to "commit or facilitate" criminal copyright and trademark infringement.[247] The warrant alleged that Rojadirecta committed *and* facilitated criminal copyright infringement.[248] Rojadirecta challenged the seizures in court, arguing that they violate both § 2323(a) and the First Amendment.[249] In its pleadings, the government offered two theories to justify its seizures under § 2323(a). The first was that Rojadirecta directly committed criminal infringement.[250] The second was that Rojadirecta *facilitated* criminal infringement. Under the latter approach, the government argued that Rojadirecta's criminal liability is irrelevant to the question of whether Rojadirecta facilitated infringement.[251]

Although both theories require underlying criminal infringement, they differ dramatically in terms of what the government must establish before seizing a domain name. The first theory requires a reasonable belief that *Rojadirecta* is committing a crime. The second, by contrast, requires a reasonable belief that *anyone Rojadirecta links to* is committing a crime. Below, I argue that both theories embrace novel statutory interpretations that effectively expand the government's enforcement authority in uncertain ways.

---

247 18 U.S.C. § 2323(a) (2012). The seizure was part of a larger ICE initiative called "Operation in Our Sites" under which ICE has seized hundreds of domain names associated with copyright and trademark infringement and counterfeiting. Bryce Baschuk, *ICE Domain Seizures Curb Counterfeit Sales on Cyber Monday*, WASH. INTERNET DAILY, Nov. 29, 2011.

248 *Rojadirecta* Affidavit, *supra* note 36, at 45.

249 Prior to the government's abandonment of the case, there were two parallel legal proceedings relating to this seizure. The first is Puerto 80's (the owner of Rojadirecta) petition to release its domain name. Puerto 80 Projects S.L.U. v. United States, No. 11 CIV 03983 (S.D.N.Y. June 13, 2011). This proceeding has been appealed to the Second Circuit. Puerto 80 Projects S.L.U. v. United States, No. 11 CIV 03390 (2d Cir. Sept. 16, 2011). The second involves the government's motion for permanent forfeiture of the domain name. United States v. Rojadirecta.org, No. 11-cv-4139 (S.D.N.Y. June 17, 2011) Because both proceedings raise similar legal issues, I combine them in the analysis below.

250 *See, e.g.*, Government's Memorandum of Law in Opposition to Petition of Puerto 80 Projects, S.L.U. Seeking Release of Seized Property Pursuant to 18 U.S.C. § 983(f) at 19, Puerto 80 Projects S.L.U. v. United States, No. 11-cv-3983 (S.D.N.Y. July 11, 2011) [hereinafter Government's Opposition to Puerto 80's Initial Petition] ("Puerto 80 has engaged in repeated acts of infringement . . . . ").

251 Government's Memorandum of Law in Opposition to Claimant Puerto 80 Projects, S.L.U.'s Motion to Dismiss the Amended Complaint at 1, 9, United States v. Rojadirecta.org, No. 1:11-CV-04 (S.D.N.Y. Apr. 16, 2012) [hereinafter Government's 2012 Opposition] ("Puerto 80's assertion that it is not itself directly liable . . . is wholly beside the point and utterly irrelevant . . . .").

a. Direct Criminal Infringement

As noted earlier, a longstanding line of precedent establishes that "merely linking" to third-party content is not sufficient to establish infringement.[252] The government, however, raised two arguments that potentially undermine this precedent. The first is that mere linking can constitute "aiding and abetting" criminal infringement.[253] As first-year law students learn, this is the language of accomplice liability, which the law views as equivalent to committing the underlying crime itself. The second argument is that platforms can directly infringe by *organizing* links in certain ways. Because Rojadirecta organized its links by category, the government argued that it did more than "merely link," which distinguishes the case from the earlier precedent.[254]

The potential benefits of these arguments become clear when viewed as an attempt to increase the scope of the criminal statute. Indeed, either argument, if accepted as *possible*, would blur the bright-line rule that linking itself cannot constitute infringement. For instance, the mere possibility that linking can result in accomplice liability would give the government significant leverage over any site that links to third-party content. The government would enjoy similar benefits from a holding that merely organizing links could be criminal. Most aggregation sites are not simply blank pages with lists of links—they all organize links to some extent. It would therefore be easy to point to a minimum threshold of "organization" to justify a domain name seizure.

The Rojadirecta proceedings illustrate how the broader standard might work in practice. In one of the hearings, the government specifically addressed the concern that its preferred standard would lead to a "doomsday scenario" of shutting down sites like Google. The government clarified that, although the statutory language is "broad," the connection between the linking site and third-party content has to be "more than de minimis." Google, it explained, is not "substantially connected" enough to infringe.[255] Although the government's argument was seemingly narrow, *its preferred standard* was quite broad. Specifically, it would necessarily require a fact-intensive inquiry regarding the degree of the "connection" between the linking sites and the third-party content. Thus, even if the government had lost this

252 *See supra* note 197.

253 Government's Opposition to Puerto 80's Initial Petition, *supra* note 250, at 17, 21 (stating that Rojadirecta has "aided and abetted the infringement by others").

254 Government's Memorandum of Law in Opposition to the Motion by Claimant Puerto 80 Projects, S.L.U. to Dismiss the Verified Complaint at 12 n.7, United States v. Rojadirecta.org, No. 11-cv-4139 (S.D.N.Y. Aug. 26, 2011) [hereinafter Government's 2011 Opposition].

255 Transcript of Hearing at 31–32, United States v. Rojadirecta.org, No. 11-cv-4139 (S.D.N.Y. Dec. 6, 2011).

particular case on the merits, the standard—if accepted—would have increased leverage against future defendants.

At other times, the government arguably implied that Rojodirecta's *secondary* liability could itself be criminal predicate act to trigger domain name seizures under § 2323(a).[256] This interpretation would also significantly expand criminal liability doctrine. As noted earlier, the Copyright Act of 1976 does not expressly define secondary liability. Instead, the statute implicitly endorses the judicially created secondary liability that predated the statute by decades.[257] Because secondary liability is not expressly defined, Rojadirecta argued that it cannot be a crime, and therefore cannot provide the predicate act for a § 2323 seizure.[258] At the very least, relying on these provisions of the Copyright Act to establish criminal secondary liability would raise significant notice and due process concerns.[259]

If, however, a court ever held that secondary liability could be criminal, it would significantly increase the scope of public enforcement authority. Under this reading, criminal statutes would be "pegged" to civil secondary liability doctrines. And as those doctrines expand and became more uncertain, they would necessarily enlarge the scope of criminal statutes as well.

One final dispute in the Rojadirecta proceeding was the proper definition of "willfulness." Unlike the strict liability regime of civil copyright law, criminal copyright statutes require that defendants act "willfully." While courts have not always been clear, the general consensus is that willfulness requires the government to show specific intent, a subjective standard.[260] In its pleadings, however, the government urged a more objective standard that includes a "reckless disregard" of infringing activity.[261] I do not provide a comprehensive analysis of willfulness here. For purposes here, the point is that the government preferred a broader standard that would potentially cover a wider range of activity.

---

256 In some pleadings, for instance, the government argued that the required "infringing acts" were present because Rojadirecta "has engaged in contributory infringement." Government's Opposition to Puerto 80's Initial Petition, *supra* note 250, at 18–22.

257 *See supra* note 168. On the doctrine's common-law origins, see Högberg, *supra* note 149, at 913–15; and Alfred C. Yen, *A First Amendment Perspective on the Construction of Third-Party Copyright Liability*, 50 B.C. L. REV. 1481, 1485 (2009).

258 Memorandum of Points and Authorities in Support of Claimant's Motion to Dismiss at 8–9, United States v. Rojadirecta.org, No. 11-cv-4139 (S.D.N.Y. Aug. 5, 2011) [hereinafter Puerto 80 Motion to Dismiss]. Rojadirecta also noted it was aware of no cases in which anyone had ever been charged with criminal secondary liability. *Id.*

259 As an aside, these concerns illustrate the benefits of alleging accomplice liability—it provides a backdoor way of effectively criminalizing secondary liability by classifying it as direct infringement.

260 Julie L. Ross, *A Generation of Racketeers? Eliminating Civil RICO Liability for Copyright Infringement*, 13 VAND. J. ENT. & TECH. L. 55, 85 (2010).

261 Government's 2011 Opposition, *supra* note 254, at 14–15.

b. Facilitation of Infringement

In addition to alleging direct infringement, the government has alleged in other pleadings that Rojadirecta's criminal liability is irrelevant to the legality of the seizure under § 2323(a).[262] Under this theory, the government may seize domain names that facilitate infringement even if the website itself is not infringing at all. To satisfy this standard, the government must establish a reasonable belief that criminal activity is occurring *somewhere* and that the website facilitated it in some way (for instance, by linking to it). This requirement is easier to establish because it does not require establishing criminal activity by the linking website itself.

This interpretation of § 2323(a) avoids many of the expansions of the criminal statutes themselves discussed above. It does, however, dramatically expand the concept of "facilitation" under § 2323(a). As Rojadirecta argued, the government's theory attempts to "disaggregate seizure from any allegation of wrongdoing."[263] If wrongdoing is no longer required, it is—as Rojadirecta argues—difficult to find coherent limits to the government's seizure authority.[264] For instance, under this interpretation, the statute arguably justifies the seizure of popular search engines, computer software, or even the physical access infrastructure that transmits data across the network. While the government would deny any intention to pursue these third parties, the decision would—under this interpretation—remain within its discretion.

In sum, both of the government's theories expand enforcement authority in uncertain ways. If the government alleges that Rojadirecta directly infringed, its theory requires expansive interpretations of various criminal law statutes and doctrine. If, by contrast, the government alleges that infringement is irrelevant to facilitation, then it expands § 2323(a) in an even more expansive manner.

B. *SOPA and PIPA*

The 112th Congress considered legislation designed to combat infringement by foreign websites. The House's version was called the Stop Online Piracy Act (SOPA),[265] while the Senate's was the Protect IP

---

262 *See supra* note 251.

263 Claimant Puerto 80 Projects, S.L.U.'s Reply to Government's Memorandum of Law in Opposition to the Motion to Dismiss the Verified Complaint at 1–2, United States v. Rojadirecta.org, No. 11-cv-4139 (S.D.N.Y. Sept. 2, 2011).

264 *Id.*

265 Stop Online Piracy Act (SOPA), H.R. 3261, 112th Cong. (2012).

Act of 2011 (PIPA).[266] Congress ultimately dropped both bills in the face of intense controversy, but the bills will likely be revisited in future congressional sessions.[267] The bills' purpose was to target infringement by foreign sites currently beyond the reach of domestic copyright law. Both bills, however, attracted criticism by targeting these sites *indirectly* through third-party intermediaries.[268] Specifically, both bills created obligations for—and enforcement remedies against—Internet Service Providers (ISPs), search engines, payment processors, and online advertisers.[269]

While the bills generated no shortage of commentary, my focus is on how SOPA and PIPA can be understood as attempts to create broad legal uncertainty for Internet platforms and other third-party intermediaries. Indeed, the bills are consciously designed to force platforms to assume enforcement costs to avoid the risk of liability. In this respect, SOPA and PIPA represent Congress's most aggressive attempt to outsource copyright enforcement costs to third-party Internet platforms.

Although SOPA and PIPA expand both private and public enforcement authority, I focus here only on the public enforcement provisions.[270] To begin, both bills authorize in personam enforcement actions against the owner, operator, or registrant of a foreign infringing website, which is a defined term. If the government cannot locate these parties (which would presumably be common with foreign sites), the bills authorize in rem proceedings against the sites or their domain names.[271] In this respect, the bills extend § 2323(a) seizure authority to foreign-based websites. Critically, the bills also allow the government to simultaneously require the third-party intermediaries listed above to restrict payments and access to the site. If the intermediaries fail to comply, the government can pursue injunctive actions against them.[272]

These various provisions, if enacted, would increase uncertainty in several different respects. First, SOPA and PIPA do not clearly define "infringing" sites. Of the two, the original SOPA language is the more expansive. It defines a "foreign infringing site" as a site "committing or facilitating" criminal violations of copyright and trademark law.[273] This

266 Protect IP Act of 2011 (PIPA), S. 968, 112th Cong. (2012).

267 Timothy B. Lee, *Slow Learner? MPAA Chief Hints at Talks to Revive SOPA*, ARS TECHNICA (Apr. 5, 2012), http://arstechnica.com/tech-policy/2012/04/slow-learner-mpaa-chief-hints-at-talks-to-revive-sopa; Somini Sengupta, *Big Victory on Internet Buoys Lobby*, N.Y. TIMES, Jan. 27, 2012, at B1.

268 Amy Chozick, *Tech and Media Elite Are Likely to Debate Piracy*, N.Y. TIMES, July 10, 2012, at B1.

269 SOPA, H.R. 3261 §§ 102(c)(2), 103(b); PIPA, S. 968 §§ 3(d)(2), 4(d)(2).

270 SOPA, H.R. 3261 § 102; PIPA, S. 968 § 3.

271 SOPA, H.R. 3261 § 102(b); PIPA, S. 968 § 3(a).

272 SOPA, H.R. 3261 § 102(c)(4); PIPA, S. 968 § 3(e).

273 SOPA, H.R. 3261 § 102(a).

language is virtually identical to the statutory text in § 2323(a).[274] By copying this language, SOPA potentially imports the same expansive interpretations of "facilitation" that the government has used in the domain seizure cases.[275]

Another source of uncertainty is that the bills provide little guidance on how intermediaries can satisfy their obligations following a government demand. For instance, both PIPA and the original SOPA language require intermediaries to take "technically feasible and reasonable measures" to prevent users from locating and accessing infringing sites identified by the government.[276] The scope of these requirements, however, is unclear. While ISPs are required to take certain steps (such as blocking domain name resolution), SOPA does not provide that these steps *satisfy* the requirement.[277] Thus, as originally written, the bill contemplates that other unnamed measures could also be required. In terms of time, PIPA and the SOPA Manager's Amendment (a revised version of SOPA released in response to criticism) require intermediaries to comply "as expeditiously as possible."[278]

The original SOPA bill also potentially imposes an affirmative duty upon ISPs and search engines to monitor their networks for infringement. SOPA explicitly states that *pay processors* and *advertisers* have "[n]o duty to monitor."[279] The textual implication is that other intermediaries (namely, ISPs and search engines) *do* have such a duty. In this respect, SOPA's requirements are dramatically broader than the DMCA safe harbor, which expressly rejects an affirmative duty to monitor.[280]

Interestingly, SOPA and PIPA do create certainty for intermediaries so long as they comply with government requests. Both provisions create a broad safe harbor from litigation arising from actions that intermediaries take in response to government requests.[281] The clarity of the safe harbor, however, does not apply to intermediaries who believe the requests are invalid or overbroad. Instead, intermediaries objecting to government requests must affirmatively establish that they lack "technical means" to comply without "incurring

---

274 *Compare* 18 U.S.C. § 2323(a)(1)(A)–(B) (2012), *with* SOPA, H.R. 3261 § 102(a).

275 This expansive concept remained in the proposed revision of SOPA (called the "Manager's Amendment"). Although the Manager's Amendment dropped the term "facilitation," the change was largely cosmetic because it continued to define "foreign infringing sites" in terms of § 2323(a). Amendment in the Nature of a Substitute to H.R. 3261 § 102(a) (2011).

276 SOPA, H.R. 3261 § 102(c)(2); PIPA, S. 968 § 3(d)(2).

277 SOPA, H.R. 3261 § 102(c)(2)(A).

278 Amendment in the Nature of a Substitute to H.R. 3261 § 102(a) (2011).

279 SOPA, H.R. 3261 § 102(c)(2)(C)–(D).

280 17 U.S.C. § 512(m)(1) (2012).

281 SOPA, H.R. 3261 § 102(c)(5); PIPA, S. 968 § 3(d)(5).

an unreasonable economic burden."[282] Collectively, these provisions create clear incentives to comply with all government requests. Removing content from their networks provides broad immunity, while rejecting government demands requires establishing an affirmative defense defined as a fact-specific standard. For most platforms, it would not be a difficult choice.

In sum, SOPA and PIPA—if enacted—would create a cloud of uncertainty that would significantly increase the scope of public enforcement authority.[283] This expanded authority, in turn, would lead to higher compliance costs, and would create incentives for Internet platforms to affirmatively police their networks. As a result, the mere existence of SOPA and PIPA would allow the government to outsource copyright enforcement to Internet platforms by implied threat even if the government never pursued a single enforcement action.

C. *Criminal Prosecution*

The government's recent criminal prosecutions of Internet platforms are perhaps its most effective means of influencing behavior by creating uncertainty.[284] As noted earlier, the threat of criminal liability is qualitatively different than other enforcement remedies. The risk of jail arguably creates different incentives than purely financial penalties. And unsurprisingly, several cyberlockers quickly changed their business practices following the government's indictment and *arrest* of Megaupload employees.[285] Accordingly, this Section examines both the expansion of criminal prosecution and the subsequent reactions of Internet platforms.

The recent expansion of criminal copyright liability has resulted from both an increase in criminal statutes, and from broad interpretations of existing statutes. The literature has documented the growth of criminal copyright statutes over the past 15 years.[286] My focus, however, is on novel interpretations of existing criminal statutes. These interpretations are illustrated by the recent indictments and arrests of the owners of Megaupload (a cyberlocker) and TVShack (a linking site).

---

282 SOPA, H.R. 3261 § 102(c)(4); PIPA, S. 968 § 3(e).

283 Michael Masnick, *The Definitive Post on Why SOPA and Protect IP Are Bad, Bad, Ideas*, TECHDIRT (Nov. 22, 2011), http://www.techdirt.com/articles/20111122/04254316872/definitive-post-why-sopa-protect-ip-are-bad-bad-ideas.shtml (noting uncertainty created for "nearly every site online").

284 Corwin, *supra* note 8 (arguing that the Megaupload indictment is more influential than SOPA and PIPA).

285 *See supra* notes 66–67.

286 *See, e.g.*, Irina D. Manta, *The Puzzle of Criminal Sanctions for Intellectual Property Infringement*, 24 HARV. J.L. & TECH. 469, 481–85 (2011) (illustrating expansion of criminal statutes).

To review, Megaupload is a cyberlocker that stores files uploaded by its users, who could then share the files with the public.[287] The government alleges that Megaupload is not a passive storage company, but instead actively encourages and facilitates massive copyright infringement.[288] According to prosecutors, one of Megaupload's more problematic actions is paying users whose files were most often downloaded. Their allegation is that these files were copies of popular movies and albums.[289] To be clear, I take no position on whether Megaupload's business practices were completely legal—indeed, some practices may prove to be criminal. My argument, however, is that certain aspects of the Megaupload prosecution expand the traditional boundaries of criminal liability in ways that make its scope more uncertain.

The primary criticism of the Megaupload indictment is that it applies criminal law to conduct traditionally treated as civil infringement.[290] While the indictment alleges that Megaupload employees uploaded pre-release versions of movies—a clear crime—the thrust of the government's case involves punishing Megaupload for the acts of its *users*.[291] Traditionally, however, these actions are governed by civil secondary liability doctrines.[292] And because those doctrines are common law creations not fully defined by the Copyright Act, they arguably cannot establish criminal liability.[293]

The government's indictment also expands the criminal statute in more specific ways. Specifically, the government justifies its indictment by listing several legitimate business practices that UGC platforms commonly use. These practices include providing advertisements, offering premium subscriptions, deleting inactive files, and removing links to infringing files rather than removing all identical copies of the

287 Sisario, *supra* note 6.

288 *Megaupload* Indictment, *supra* note 25, ¶ 2.

289 *Id.* at ¶ 5.

290 Anthony Falzone & Jennifer Granick, *Megaupload.com Indictment Leaves Everyone Guessing—Part I*, DAILY JOURNAL, Mar. 14, 2012, *available at* http://cyberlaw.stanford.edu/publications/megauploadcom-indictment-leaves-everyone-guessing-part-1 ("[T]he indictment pushes several aspects of copyright law well past existing boundaries."); Eric Goldman, *Comments on the Megaupload Prosecution*, TECH. & MKT'G LAW BLOG (Apr. 30, 2012, 9:30 AM) http://blog.ericgoldman.org/archives/2012/04/megaupload.htm ("The government is using its enforcement powers to accomplish what most copyright owners haven't been willing to do in civil court.").

291 Jennifer Granick, *Megaupload: A Lot Less Guilty Than You Think*, CIS BLOG (Jan. 26, 2012, 11:47 AM), http://cyberlaw.stanford.edu/node/6795 ("The heart of this case is whether and when an enterprise can be held criminally liable for the conduct of its users.").

292 For instance, Yochai Benkler expressed surprise at "how aggressive the move is [and] how much it uses extensions of criminal law enforcement and copyright liability." Corwin, *supra* note 8 (quoting Yochai Benkler, Professor, Harvard University).

293 *See supra* note 258.

files.[294] Indeed, courts have recently held that the latter practice—removing only the link—could not justify *civil* infringement.[295]

Further, although the criminal statute requires "willfulness," the government cites various actions arguably demonstrating just the opposite. For instance, the indictment states that Megaupload disabled its search functionality to "conceal the scope of its infringement."[296] This disabling, however, could just as easily be described as an infringement prevention strategy that would defeat specific intent.[297]

The government's prosecution of the owner of TVShack arguably expands criminal liability even further.[298] TVShack is a website that provides links to television content stored on third-party servers. The site is hosted in Sweden, and was founded by Richard O'Dwyer, a 24-year-old UK citizen. TVShack called itself a resource site that did not host any content itself.[299] Much of the content to which it linked, however, was infringing. In 2010, ICE seized the site's domain name, and the government later indicted O'Dwyer in American federal court, and the United States requested that O'Dwyer be extradited to the United States for prosecution.[300] In late 2012, O'Dwyer ultimately agreed to a deferred prosecution agreement, which provides that the United States will drop the case if he pays a fine and does not violate United States laws.[301]

The TVShack prosecution potentially expands criminal liability by alleging that *linking* to third-party content can trigger prosecution. Although TVShack admittedly linked to infringing content, no one alleged that the site itself stored that content.[302] The government's theory implied that linking can justify criminal prosecution. As noted earlier, however, courts have consistently held that mere linking cannot provide a basis for *civil* liability.[303] In this respect, the TVShack prosecution threatened to extend enforcement authority a step beyond

---

294 *Megaupload* Indictment, *supra* note 25, ¶¶ 4–23. For instance, James Grimmelmann observes "much of what the indictment details are legitimate business strategies many websites use to increase their traffic and revenues." Corwin, *supra* note 8.

295 Capitol Records, Inc. v. MP3Tunes, LLC, 821 F. Supp. 2d 627, 639 (S.D.N.Y. 2011).

296 *Megaupload* Indictment, *supra* note 25, ¶ 10.

297 Falzone & Granick, *supra* note 290 ("The indictment identifies a number of steps Megaupload took that appear designed to reduce rather than induce piracy.").

298 Somini Sengupta, *U.S. Pursuing a Middleman in Web Piracy*, N.Y. TIMES, July 13, 2012, at A1 (providing overview of TVShack's history and founder).

299 *Id.* ("Mr. O'Dwyer's backers say his site was effectively a search engine.").

300 *Id.*; *see also* Nate Anderson, *Copyright Wars Heat Up*, ARS TECHNICA (Mar. 13, 2012), http://arstechnica.com/tech-policy/2012/03/copyright-wars-heat-up-us-wins-extradition-of-college-kid-from-england.

301 *Richard O'Dwyer "Happy" US Copyright Case Is Over*, BBC NEWS (Dec. 6, 2012), http://www.bbc.co.uk/news/uk-england-20636626.

302 Anderson, *supra* note 300 ("O'Dwyer's site was a 'linking site' that did not host infringing content itself.").

303 *See supra* note 197.

the domain name seizures, in which linking merely provided a "reasonable basis" for § 2323(a) forfeiture proceedings.

The net effect of these prosecutions is to cast a shadow of uncertainty upon a wide range of common business practices. From the government's perspective, however, this uncertainty offers several benefits. First, it allows the government to initiate more criminal prosecutions. In many instances, the cost of the prosecution itself can destroy a company even if it is ultimately acquitted. In Megaupload's case, the government not only arrested the employees, it also seized its servers and prevented customers from accessing their own files.[304] In this respect, the government threatened cyberlockers by making *customers* more wary of using them.

Second, the uncertainty will create significant incentives for similar companies—particularly cyberlockers—to change their practices, even if those practices are efficient and legal. In this respect, the Megaupload prosecution has succeeded even if the case is ultimately dismissed. Immediately following the arrest, and as noted earlier, several popular cyberlockers changed their services to avoid the risk.[305] Finally, as the risk of criminal liability increases, Internet platforms will have more difficulty obtaining investment and hiring top talent—or at minimum, will have to pay more for them. As Granick and Falzone write, "entrepreneurs . . . are not going to invest their time and money . . . if guessing wrong means financial ruin and jail time."[306]

IV. NORMATIVE ANALYSIS OF EXPANDED UNCERTAINTY

The previous Parts explore how increased uncertainty effectively extends the scope of secondary copyright liability in both the civil and criminal contexts.[307] It is not obvious, however, that this extension is normatively harmful. In many contexts, broad secondary liability is sound policy. This Part, accordingly, examines the policy tradeoffs of secondary liability as a general matter. It then explains—in light of these tradeoffs—why broad secondary liability is inappropriate for Internet platforms. Specifically, it argues that Internet platforms provide unique

304 Geoffrey A. Fowler & Devlin Barrett, *Talks Consider Access to Megaupload Files*, WALL ST. J., Jan. 31, 2012, http://online.wsj.com/article/SB10001424052970203920204577195340316406190.html.

305 *See supra* notes 66–67.

306 Anthony Falzone & Jennifer Granick, *Megaupload.com Indictment Leaves Everyone Guessing—Part II*, DAILY JOURNAL, Apr. 6, 2012, *available at* http://cyberlaw.stanford.edu/publications/megaupload-indictment-leaves-everyone-guessing-part-2.

307 Technically, there is no such thing as criminal secondary liability. I use the term in a broader sense because the criminal enforcement actions generally arise from the actions of a platform's users. *See supra* note 291.

levels of economic and social spillovers that would be threatened by broad and unclear liability.

A. *Policy Tradeoffs of Secondary Liability*

Secondary liability—like copyright law more generally—involves policy tradeoffs.[308] Broad liability protects rights owners at the cost of threatening legitimate activity. Narrow liability, by contrast, protects legitimate activity at the cost of tolerating some level of infringement. The appropriate balance depends on the circumstances in which secondary liability is being applied. The challenge, then, is to identify the conditions in which secondary liability provides the most benefits—as well as those in which it causes the most harm.

The primary benefit of secondary liability is that it provides a more efficient way to enforce copyright protections. These benefits are especially evident when the administrative costs of pursuing individual infringers are high, and when the secondary party can more cheaply prevent the infringement from occurring.[309] In these contexts, copyright owners can pursue a single enforcement action instead of thousands of individual ones. Such targeted actions not only lower litigation costs, they also modify a wider range of infringing conduct at lower cost. Secondary liability also deters future infringement by creating incentives for third-party facilitators to monitor for—and prevent—infringement by their users.[310] The more cheaply that facilitators can prevent the infringement in the first place, the more justified secondary liability becomes. In addition, enhanced secondary liability creates demand for—and incentives to create—new technologies that help companies locate and remove infringing material.[311]

In addition to increasing efficiency, secondary liability also promotes fairness.[312] If third-party facilitators are benefiting from users' infringement, the doctrine ensures that copyright owners will be compensated and that facilitators will internalize the costs of the infringement they enable. Further, third party facilitators often possess

---

308 For a good overview of the policies underlying secondary liability generally, see Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395 (2003).

309 *Id.* at 396–97; Neil Weinstock Netanel, *Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing*, 17 HARV. J.L. & TECH. 1, 16 (2003) ("[I]mposing third-party liability can be an efficient mechanism for enforcing legal rules in many areas, including copyright.").

310 Grossman, *supra* note 148, at 365–67; Helman & Parchomovsky, *supra* note 18, at 1200–04.

311 Helman & Parchomovsky, *supra* note 18, at 1203–04.

312 Grossman, *supra* note 148, at 365–66 ("Simple fairness is arguably the overarching purpose of the rules.").

greater financial resources than individual infringers.[313] Secondary liability can therefore help ensure that copyright owners will be compensated appropriately.

Secondary liability, however, can impose substantial costs as well. In general, the more that secondary liability threatens non-infringing activity, the more its costs grow.[314] Indeed, one problem of applying secondary liability to general-purpose technologies is that they necessarily include both infringing and non-infringing uses. In this respect, secondary liability actions create negative externalities by imposing costs on the innocent parties whose non-infringing activity is jeopardized.[315] The higher these externalities, the less compelling secondary liability becomes.

In light of these considerations, some scholars have proposed a negligence-like welfarist framework to determine when secondary liability is appropriate. For instance, Lichtman and Landes have proposed considering the following factors in determining whether contributory liability is appropriate: the costs of direct infringement; the benefits of other lawful use; the costs of modifying behavior; and the efficiency gains that liability would create.[316] The basic idea is that secondary liability is most justified when it can lower the costs of effective enforcement, and least justified when it imposes significant negative externalities on third parties.

B. Secondary Liability and Internet Platforms

In this Section, I argue that secondary liability imposes more costs than benefits when applied to Internet platforms. My premise is that Internet platforms have unique economic and technological characteristics that justify narrow application of secondary liability doctrines.

The central argument supporting this position is that secondary liability actions will necessarily be overbroad when applied to Internet platforms such as UGC and information location sites. This overbroad application imposes negative externalities upon platforms and society as a whole. Importantly, platforms cannot completely capture the benefits of the content they generate.[317] Further, the marginal cost of removing

313 *See, e.g.*, Lynda J. Oswald, *International Issues in Secondary Liability for Intellectual Property Rights Infringement*, 45 AM. BUS. L.J. 247, 250 (2008).

314 Lichtman & Landes, *supra* note 308, at 397.

315 Netanel, *supra* note 309, at 16–17.

316 Lichtman & Landes, *supra* note 308, at 398.

317 Lemley, *supra* note 145, at 112 ("Intermediaries do not and cannot reasonably expect to capture anything like the full social value of the uses that pass through their system."); Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the*

an individual user or file pales in comparison to the costs of copyright liability. Together, these cost structures create incentives to liberally filter or remove legitimate content.[318] This response is problematic, however, given that platforms are general-purpose technologies that inevitably include both infringing and non-infringing uses. And because Internet platforms are capable of generating uniquely high levels of non-infringing and expressive activity, the negative externalities that secondary liability creates are significant.

To begin, broad secondary liability for Internet platforms threatens a wide range of innovation. As recent communications law scholars have observed, low entry costs are an important source of innovation.[319] The lower the entry costs, the more new entrants a market can expect. As entrants increase, so too do the chances of innovative new services. In this respect, Internet platforms are uniquely capable of generating a substantial range of innovative content and applications.[320] YouTube, for instance, dramatically lowers the costs of creating and uploading video. These economic and technological characteristics are the source of the site's wide diversity of content. Similarly, cyberlockers lower the costs of distribution and storage—particularly for large video and audio files. These reduced costs enable novel and diverse uses.

Secondary liability also threatens *future* sources of innovation. Applying the doctrine to new startups threatens the unpredictable benefits the platforms will eventually provide. As Julian Sanchez has observed, the fact that these platforms are *user*-driven makes innovation occur more rapidly and in more unexpected ways.[321] He notes that Twitter evolved from a stream of mundane status updates into a communications tool that helped topple dictators in the Middle East. Similarly, the YouTube of 2005—which included vast amounts of infringing material—differs significantly from today's YouTube, which boasts professional content and advanced copyright monitoring systems. Critically, Sanchez traces this innovation back to the inherent "generative" technological characteristics of the platform itself—characteristics it shares with the Internet more generally:

> On the Internet, you don't know what a new technology is for until

First Amendment, 24 HARV. J.L. & TECH. 171, 185 (2010).

318 Helman & Parchomovsky, *supra* note 18, at 1207–09; Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 28–39 (2006); Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Immunity*, 87 NOTRE DAME L. REV. 293, 301–03 (2011).

319 For a comprehensive summary, see generally BARBARA VAN SCHEWICK, INTERNET ARCHITECTURE AND INNOVATION (2010).

320 *Id.* at 204–13 (discussing examples of relatively low cost innovation).

321 Julian Sanchez, *Infringement and Innovation in Online Platforms*, NOTES FROM THE LOUNGE (Jan. 24, 2012), http://www.juliansanchez.com/2012/01/24/infringement-and-innovation-in-online-platforms.

> you see what people do with it . . . . [A]nd the most interesting uses the users find for your platform won't necessarily be the ones you intended. Indeed, that's the guiding idea behind the "end to end principle" that has made the meta-platform of the Internet itself so incredibly generative.[322]

The same generative principles that allow the Internet to create innovation allow Internet platforms to do the same—albeit on a smaller scale.

Secondary liability for platforms also threatens a wide range of constitutionally protected expression.[323] Although there is theoretical tension between copyright law and the First Amendment, courts have uniformly recognized that infringement is not protected speech.[324] The difference with Internet platforms, however, is that they host a wide range of legal *user-created* expression as well. Applying broad secondary liability to platforms endangers protected speech in ways that infringement actions against more traditional defendants do not. Some scholars have referred to these threats as "censorship by proxy" in that it allows private parties to limit expression in ways government cannot.[325]

Secondary liability is also likely to be overbroad if it effectively shifts the burden of monitoring and enforcement to platforms. Comparatively, platforms are less suited than content owners to determine whether an individual activity is infringing or not.[326] For one, Internet platforms host an enormous and ever-changing amount of files.[327] Further, it is often impossible for platforms to distinguish between infringing and non-infringing uses.[328] For instance, two identical files stored on a platform's server may be treated differently under copyright law. One file might be standard infringing activity, while another might be licensed promotional content or fair use (e.g., if a news organization or copyright law professor posted it).

Accordingly, the practical effect of shifting enforcement costs to platforms will be overbroad removal of content. Platform owners operating under uncertain secondary liability standards would have

---

322 *Id.*; *see also* Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974 (2006).

323 Helman & Parchomovsky, *supra* note 18, at 1208–09.

324 Sony Music Entm't Inc. v. Does 1–40, 326 F. Supp. 2d 556, 562–63 (S.D.N.Y. 2004) ("The First Amendment . . . does not protect copyright infringement.").

325 Kreimer, *supra* note 318, at 16–17; Seltzer, *supra* note 317, at 177–79; Wu, *supra* note 318, at 295–98.

326 UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1037 (9th Cir. 2011) ("Copyright holders know precisely what materials they own, and are thus better able to efficiently identify infringing copies than service providers like Veoh."), *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL 1092793 (9th Cir. Mar. 14, 2013).

327 Lemley, *supra* note 145, at 101–02 ("Google has no realistic way of knowing which of the over 10 billion [w]eb pages it searches might have information on it that violates the rights of someone else.").

328 Helman & Parchomovsky, *supra* note 18, at 1211.

incentives to remove any material that copyright owners have identified—or *may identify*—as infringing. Indeed, one critique of the DMCA is that platform owners already comply uncritically with content owners' takedown requests.[329] If the safe harbor becomes more uncertain, rational platforms will be even more aggressive in removing potentially infringing content.[330]

Of course, copyright owners can object that the sheer volume of files makes it prohibitively costly for them to monitor platforms as well.[331] This objection is valid, and the problem of monitoring costs cannot be avoided altogether. Someone has to do it. On balance, however, I argue that the burden should fall on the content owner. Placing the burden with content owners will force them to internalize the costs of enforcement proceedings. Content owners will therefore allocate their resources toward those activities that are most harmful and most clearly infringing. If, by contrast, content owners can outsource enforcement to platforms, they have few incentives to refrain from aggressive and overbroad removal efforts that threaten innovation and speech in the manner discussed above.

Finally, it is unclear whether secondary liability would actually prevent infringement in a more efficient way. Individual Internet platforms—unlike certain facilitating technologies in the past—do not provide an exclusive or "bottleneck" means to infringe copyright. If one platform for infringement vanishes, another will take its place. If, by contrast, content owners had effectively killed the VCR, they might well have prevented infringement of television content for years. The distinction traces back to the openness of the Internet itself—so long as people can exchange information on the Internet, it will be difficult to prevent infringement by shutting down any one platform. Shutting down an individual platform, however, would impose other types of costs given that platforms are not all similarly innovative and expression-creating.

V. HOW TO BETTER PROTECT INTERNET PLATFORMS

In this Part, I propose measures to protect Internet platforms from uncertain secondary liability. Although I would welcome new clarifying

---

329 Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1888 (2000) (stating that the DMCA "encourage[s] ISPs to indiscriminately remove material from the Internet").

330 *See* Gibson, *supra* note 18, at 887–95 (noting how the combination of legal uncertainty and risk averseness effectively lead to expansion of the breadth of liability).

331 Opening Brief of Plaintiffs-Appellants at 31, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012) (No. 10-3270), 2010 WL 5066007, at *31 ("The consequences of the lower court's view would be to have every copyright owner search every site on the Internet.").

legislation, my proposals do not require it. Instead, courts can generally implement these measures through interpretations of existing law. The principal theme uniting them is that courts should narrow and clarify legal uncertainty for Internet platforms facing enforcement actions. This Part first defends the choice of bright-line rules generally, and then applies them to both the private and public enforcement contexts.

A. *The Importance of Clear Rules*

The preceding Part illustrated why liability for Internet platforms should be *narrow*. This Section, by contrast, argues that liability should also be *clear*. Accordingly, a key policy recommendation is that secondary liability for Internet platforms generally be defined by bright-line rules with low administrative costs. Of course, the debate between rules and standards has a long and rich history in the literature, and any proposal can be met by numerous well-known objections.[332] Despite these potential objections, however, I argue that litigation against Internet platforms for secondary copyright liability possesses several characteristics that tilt the balance toward rules.

First, the frequency and nature of activity on Internet platforms supports applying rules over standards. As noted earlier, in terms of public costs, rules are more costly to create, but cheaper to apply.[333] Standards, by contrast, are easier to create but are more expensive to apply.[334] The implication is that rules are more efficient when the governed conduct is frequent and homogenous, while standards are more efficient when it is infrequent and factually dissimilar.[335] With respect to Internet platforms, these factors favor rules. The very essence of user-generated content sites is that users can easily and frequently upload and share their content. Accordingly, the content of the sites are always changing and being updated. In many instances, however, the content posted will infringe. This pattern of high volume and repeated infringement will arise again and again, even assuming sophisticated filters. Given the sheer volume of the activity, bright-line rules for secondary liability are arguably the better choice.

---

332 *See generally* Daniel A. Crane, *Rules Versus Standards in Antitrust Adjudication*, 64 WASH. & LEE L. REV. 49, 53 n.11 (2007) (providing extensive list of sources); Goldman & Parchomovsky, *supra* note 18, at 1502–03; Kaplow, *supra* note 37; Korobkin, *supra* note 37; Eric A. Posner, *Standards, Rules, and Social Norms*, 21 HARV. J.L. & PUB. POL'Y 101 (1997); Pierre J. Schlag, *Rules and Standards*, 33 UCLA L. REV. 379 (1985); Cass R. Sunstein, *Problems with Rules*, 83 CALIF. L. REV. 953 (1995).

333 *See supra* note 37.

334 Korobkin, *supra* note 332, at 31–32 ("The public costs of administering rules will tend to be front loaded, whereas the costs of administering standards will be back loaded.").

335 *Id.* at 32–34; *see also* Kaplow, *supra* note 332, at 621 ("The central factor influencing the desirability of rules and standards is the frequency with which a law will govern conduct.").

Second, assuming that Internet platforms provide unique generative benefits, it is important to not to "chill" this activity. By providing clear boundaries, rules provide the certainty necessary for innovators and investors alike. Standards, by contrast, are inherently vague in that their content is not completely defined until *after* the conduct in question has occurred.[336] As James Gibson has argued, vagueness in intellectual property law can often lead to over-deterrence of risk-averse actors.[337] While Gibson does not focus specifically upon Internet platforms, the expressive and economic value of these platforms makes over-deterrence even more problematic in this context. Further, although Gibson notes that over-deterrence leads to unnecessary licensing,[338] the enormous transactions costs involved with licensing the various content uploaded on platforms would make it very difficult for licensing agreements to occur.[339]

Like any rules, however, my proposed rules are potentially over- and underinclusive.[340] The larger concern in this context is *under*inclusiveness in that too many platforms that facilitate infringement may escape liability. Indeed, clear rules could potentially increase infringement as platforms can more clearly approach the line of liability without crossing it. More vague standards, by contrast, would create incentives to police infringement more aggressively to avoid even approaching the grey area surrounding the line of liability. This objection is valid, and advocates of rule-based approaches should acknowledge that these results are possible. The counterargument, however, is that these costs are outweighed by the benefits of generative Internet platforms for the reasons described above. In this respect, bright-line rules can be understood as a subsidy for activity that creates numerous positive spillovers.

B. *Increasing Certainty in Private Enforcement Actions*

In the private context, courts should adopt bright-line interpretations of the statutes and doctrines most relevant in secondary liability litigation. I am not necessarily arguing that secondary liability

336 Posner, *supra* note 332, at 101; Sunstein, *supra* note 332, at 964–65.

337 Gibson, *supra* note 18, at 884, 890–95 ("Combine these doctrinal gray areas and severe consequences with the risk aversion that pervades key copyright industries, and the result is a practice of securing copyright licenses even when none is needed. Better safe than sued."); *see also* Goldman & Parchomovsky, *supra* note 18, at 1497–98 ("[L]aw and economics scholars have long observed that vague standards cause overdeterrence.").

338 Gibson, *supra* note 18, at 890–95.

339 Goldman & Parchomovsky, *supra* note 18, at 1499 ("[L]icensing fails to provide a solution for cases involving high transaction costs . . . . ").

340 Sunstein, *supra* note 332, at 992–93.

doctrines themselves should be formally "different" for Internet platforms. Instead, I argue that courts should interpret the *defenses* most relevant to these platforms—the DMCA safe harbor and the *Sony* defense—as bright-line rules. These interpretations would achieve the policy objectives without requiring formal context-specific changes to traditional secondary liability doctrines.

1. Improving the DMCA Safe Harbor

The single most effective way to protect Internet platforms is to interpret the DMCA safe harbor as a series of bright-line rules with low administrative costs.[341] The rationale is that, for Internet platforms, uncertain doctrinal standards that require expensive discovery are threatening even if platforms would ultimately prevail under them. Accordingly, courts' statutory interpretations must satisfy two requirements to mitigate this threat. First, the interpretations must allow plaintiffs complying with the safe harbor to limit or halt litigation in early dispositive motions. Second, courts must adopt bright-line interpretations *uniformly* across § 512. This latter requirement is critical and warrants further explanation.

To review, the DMCA provides an affirmative defense for plaintiffs that comply with numerous formal provisions. The statute's structure puts platforms at a disadvantage in that they must satisfy *all* requirements to enjoy the safe harbor. Content owners, by contrast, need only prevail on one disputed issue to negate the defense entirely.[342] As this Article illustrates, however, content owners do not always need to prevail, they merely need to obtain a favorable statutory interpretation on a single provision that requires fact-intensive discovery. These costs alone can be sufficient to bankrupt the platform—or at least to force it to assume monitoring and enforcement costs. Thus, even if a court interprets nine of ten provisions as bright-line rules, the tenth provision can be fatal for platforms if it is uncertain enough to drive up costs. This observation explains why the Second Circuit's *YouTube* opinion—while considered by some a win for YouTube—potentially threatens future defendants.[343] In sum, courts wishing to protect platforms must interpret the DMCA as bright-line rules across the board.

---

341 Lee, *supra* note 77, at 262 ("[T]he DMCA safe harbors should be interpreted to promote clarity for private planning.").

342 *See supra* note 87 and accompanying text.

343 As noted earlier, the Second Circuit creates significant uncertainty regarding the "willful blindness" and "benefit and control" provisions of the DMCA. Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 34–35, 38 (2d Cir. 2012).

This general interpretative approach is supported by both the text and the purpose of the statute. To begin, I should note that the DMCA is not a model of textual clarity. The statute's text does not compel clear answers to these interpretative questions. Certain provisions are phrased as formal rules,[344] while others—such as the "benefit and control" provisions—are worded as equitable standards.[345] On balance, however, I argue that the statute's *overall* text and structure justify a uniform bright-line approach. Most obviously, the entire point of a safe harbor is to create clarity.[346] In addition, the DMCA includes multiple formal requirements that are specifically detailed—particularly the notice-and-takedown regime. This detailed formal structure is inconsistent with the idea that the DMCA creates a series of vague fact-intensive standards. Indeed, the DMCA's length and complexity is unnecessary if its availability turns largely on equitable considerations. In addition, several explicit textual provisions reinforce the view of the safe harbor as a set of clear bright-line obligations. The DMCA, for instance, expressly prohibits platforms from being required to affirmatively monitor their networks,[347] or to unreasonably alter their networks to accommodate copyright owners' infringement protections.[348]

This general interpretative approach is also consistent with the DMCA's purpose and legislative history. Like the text, the DMCA's legislative history is vague and contradictory in places. And while the legislative history does not compel answers to these questions, it does include a clear emphasis on creating *certainty* for Internet technologies. For instance, both the Senate and House reports repeatedly note that the safe harbor provision will provide "greater certainty" to online service providers.[349] Further, the safe harbor itself was not originally included in the early versions of the DMCA, but was drafted in response to online providers who "sought greater certainty."[350]

Examining some of the DMCA's specific provisions illustrates how this general interpretative approach would apply in practice. The first

344 17 U.S.C. § 512(c)(3) (2012) (notification procedures and requirements).

345 *Id.* § 512(c)(1)(B) (benefit and control provisions).

346 Helman & Parchomovsky, *supra* note 18, at 1207 ("[S]afe harbors, by their very nature, are supposed to provide actors with certainty."); Lee, *supra* note 77, at 262 ("An unclear 'safe harbor' is self-defeating and of no practical use."); *see also* EFF Amicus Brief, *supra* note 18, at 7–10, 2010 WL 3706522, at *7–10.

347 17 U.S.C. § 512(m)(1).

348 *Id.* § 512(i)(2)(C).

349 For examples in the Senate report, see S. REP. NO. 105-190, at 2 (1998) ("Title II will provide certainty. . . ."); *id.* at 19 ("[T]he Committee is sympathetic to the desire of such service providers to see the law clarified in this area."); *id.* at 20, 40 (stating that the safe harbor "provides greater certainty to service providers . . . ."). For examples in the House report, see H.R. REP. NO. 105-551, pt. 1, at 11 (1998) (stating that the DMCA "narrow[s] and clarif[ies] the law" regarding secondary liability).

350 H.R. REP. NO. 105-551, pt 1, at 11.

provision is the "red flag knowledge" requirement.[351] Courts should interpret this provision to require specific knowledge of specific infringing activity—just as the Ninth Circuit held in *UMG* and the district court held in *YouTube*.[352] This bright-line interpretation would go hand in hand with interpreting the notice provisions to require specific information (generally in the form of specific URLs). As courts have recognized, one source of textual support for this interpretation is that online providers must have "reasonably sufficient" information to "locate the material" to be removed.[353] Without specific knowledge created by specific notifications, it would arguably be impossible for online providers to satisfy this requirement at reasonable costs. Further, from a policy perspective, this interpretation creates certainty by assuring platforms that they can avoid liability by complying with the formal DMCA requirements and takedown notices. Vague standards that undermine this certainty—such as the Second Circuit's "willful blindness" concept[354]—should be rejected in favor of more clear requirements.

A second disputed provision is the DMCA's "control and benefit" language. This provision presents two questions for courts. First, should the DMCA's language be interpreted as co-extensive with traditional vicarious liability? If not, how should it be interpreted? On the first question, courts should interpret the statutory language—as most recent courts have—as being distinct from common law vicarious liability.[355] Textually, the provision is admittedly identical to common law vicarious liability standards. There are, however, several reasons to interpret it differently.

For one, interpreting the DMCA as co-extensive with the ever-expanding vicarious liability standard would effectively nullify the safe harbor.[356] Such a reading is arguably inconsistent with the statute's legislative history. Originally, the initial versions of § 512 explicitly provided immunity for vicarious liability. They prohibited damages for "contributory or vicarious liability" so long as the provider "does not receive a financial benefit directly attributable to the infringing activity, if the provider has the right and ability to control such activity."[357] The

---

351 17 U.S.C. § 512(c)(1)(A)(ii).

352 UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1036–38 (9th Cir. 2011), *opinion withdrawn and superseded*, Nos. 09-55902, 09-56777, 10-55732, 2013 WL 1092793 (9th Cir. Mar. 14, 2013); Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 525 (S.D.N.Y. 2010), *aff'd in part, vacated in part*, 676 F.3d 19 (2d Cir. 2012).

353 Capitol Records, Inc. v. MP3Tunes, LLC, 821 F. Supp. 2d 627, 643 (S.D.N.Y. 2011).

354 Viacom Int'l, Inc., v. YouTube, Inc., 676 F.3d 19, 34–35 (2d Cir. 2012).

355 *See supra* note 158.

356 Lee, *supra* note 77, at 236–37 (noting the "loophole" that potentially exists under this reading).

357 H.R. REP. NO. 105-551, pt. 1, at 8 (1998) (immunizing providers from damages for "contributory infringement or vicarious liability").

bill's language, however, would be nonsensical if the "benefit and control" language were interpreted as co-extensive with "vicarious liability." Under this reading, the bill would effectively state "there are no damages for vicarious liability unless there is vicarious liability." The more likely reading is that this language meant something different than vicarious liability. Indeed, this reading is supported by other portions of the legislative history, which also state that the DMCA protects against vicarious liability.[358]

Assuming the DMCA language is different from common law vicarious liability, the next question is how courts should interpret it. One option is to impose a knowledge requirement. As I argued earlier, recent opinions have adopted this requirement as an attempt to inject bright-line rules into the requirement. The critique of this approach, as the Second Circuit recognized, is that it lacks textual support.[359]

An alternative approach would be to return to the roots of vicarious liability and interpret the provision as imposing an agency requirement.[360] Specifically, courts could read this provision as applying only to principals and agents. In general, this type of relationship does not exist between Internet platforms and their users. As a result, this interpretation would not only increase certainty, it would be more consistent with the statute's text. Another approach—that some courts arguably have used—would be to focus on the text's requirement that a party must be able to control the infringing *activity*.[361] Under this approach, the ability to remove the content from the network should be irrelevant. The focus should instead be on the actual infringing act of the user. In most cases, the platform does not enjoy this level of control over its users.

Courts should also hold that the DMCA applies to claims of inducement liability. The contrary view is that the specific intent requirements of inducement necessarily create "knowledge" that negates the safe harbor.[362] In the abstract, this argument seems compelling. In practice, however, it would effectively nullify the safe harbor by creating opportunities for extended litigation and intrusive discovery. Again, one insight this Article provides is that uncertainty of the standard is as important as the ultimate result for Internet platforms. Even if most platforms would ultimately defeat inducement claims, the standard itself

358 *Id.* at 11 ("[T]he current criteria for finding contributory infringement or vicarious liability are made clearer and somewhat more difficult to satisfy.").

359 *See supra* note 163 and accompanying text.

360 Grossman, *supra* note 148, at 407–08; Högberg, *supra* note 149, at 935–36.

361 Capitol Records, Inc. v. MP3Tunes, LLC, 821 F. Supp. 2d 627, 645 (S.D.N.Y. 2011); Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1151 (N.D. Cal. 2008) ("[T]he pertinent inquiry is not whether Veoh has the right and ability to control it [sic] *system,* but rather, whether it has the right and ability to control the *infringing activity.*").

362 *See supra* note 193.

could still threaten the platform by increasing litigation costs. Accordingly, the better interpretation is that the DMCA's protections from "monetary relief" include all secondary liability claims—as recent courts have suggested.[363]

One potential objection to these various interpretations is that it immunizes virtually all bad actors from secondary liability. In response, I would emphasize that these interpretations apply to a *defense*, and not to secondary liability doctrines more generally. Further, the more infamous peer-to-peer companies have not qualified for the DMCA safe harbor defense.[364] Indeed, it is arguable that my proposals are too narrow because they do not extend to the secondary liability doctrines that apply when the DMCA is not available.

2. Improving the *Sony* Defense

Internet platforms that are ineligible for the safe harbor can also potentially rely on the *Sony* defense. As explained earlier, however, *Sony* has become less useful for defendants through time as the defense has evolved from a bright-line rule into a more amorphous standard.[365] My recommendation, accordingly, is that courts restore *Sony*'s original bright-line rule, at least for Internet platforms. A broad *Sony* defense, however, has the potential to make the DMCA safe harbor superfluous. The challenge is to broaden *Sony* in a way that maintains incentives for platforms to comply with the DMCA's requirements.

My proposal is that the *Sony* defense should be simple. If a platform is capable of substantial non-infringing uses, then the *Sony* defense should apply. *Sony* would no longer be a presumption, or a defense that requires quantifying non-infringing uses. Instead, the interpretation returns to *Sony*'s roots by requiring only that the platform be *capable* of substantial non-infringing uses. This interpretation would increase certainty and allow defendants to halt litigation in its early stages through a summary judgment motion that documents substantial non-infringing uses.

If courts accept this interpretation, the next question is how far the *Sony* defense should extend. In particular, should it defeat all claims of secondary liability, or only specific types of claims? I propose that the *Sony* defense should apply to any claim for contributory or vicarious liability. The original *Sony* opinion applied to both kinds of claims—

---

363 *See supra* notes 194–195 and accompanying text.

364 A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025 (9th Cir. 2001); Columbia Pictures Indus., Inc. v. Fung, No. CV 06-5578, 2009 WL 6355911, at *15–18 (C.D. Cal. Dec. 21, 2009), *aff'd in part as modified*, 710 F.3d 1020 (9th Cir. 2013).

365 *See supra* Part II.B.

although the Court sometimes confusingly referred to both as "vicarious liability."[366] Because these common law doctrines have expanded significantly in recent years, a more robust *Sony* defense would provide a clean and administratively simple means of protecting platforms while sidestepping the quagmire of civil secondary liability doctrines. At minimum, however, the simplified *Sony* defense should apply to contributory liability claims. This more limited application would protect general-use platforms while maintaining incentives to comply with the DMCA.

At the same time, however, I propose that the *Sony* defense should not be available for *Grokster* inducement claims. Admittedly, this position will increase legal uncertainty for platforms and potentially subject them to more expensive litigation.[367] There are, however, several grounds that support my proposal. For one, limiting *Sony* in this way strikes an appropriate balance between copyright owners and new technologies. Inducement liability was created to reach egregious infringers that traditional secondary liability doctrines arguably did not reach.[368] Applying *Sony* too broadly would effectively nullify the doctrine.

In addition, my proposal provides a way to "clean up" the confusion surrounding *Sony* that *Grokster* introduced. Inducement claims would still be available for the most flagrant offenders, while a broad *Sony* defense would be available for other types of general-purpose platforms. Exempting inducement liability is less harmful because the doctrine is more limited than other forms of secondary liability. While the doctrine admittedly creates uncertainty, it is nonetheless more constrained than contributory and vicarious liability. In addition, the continuing availability of inducement claims provides platforms with incentives to comply with the DMCA safe harbor. If courts are concerned about discovery abuse, however, they could apply heightened pleading standards for inducement claims against Internet platforms. For instance, to survive a motion to dismiss, plaintiffs might have to identify *publicly available* evidence of inducement. With respect to companies like *Napster*, *Aimster*, *Grokster*, and other more egregious offenders, significant public evidence existed of their specific intent to promote infringement.[369] This requirement would ensure that plaintiffs

366 Jay Dratler, Jr., *Common-Sense (Federal) Common Law Adrift in a Statutory Sea, or Why* Grokster *Was a Unanimous Decision*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 413, 436 (2006) (noting the Court "us[ed] 'vicarious liability' at times as a generic term for all kinds of secondary liability").

367 *See supra* notes 187–188 and accompanying text.

368 Yen, *supra* note 184, at 513–14.

369 *See, e.g.*, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 937–38 (2005).

could sue the worst offenders, while simultaneously preventing discovery abuse.

On a final note, a broader *Sony* defense could also provide courts with a way to prevent litigation that seems consciously designed to evade the spirit of the DMCA. For instance, in *UMG*, the litigation against Veoh's investors transparently attempted to evade the DMCA, which applies only to "service providers."[370] The likely intent of the litigation was to drive up litigation costs, and to dissuade investors from allocating resources to these types of platforms. A robust *Sony* defense would provide an administratively simple means of rejecting these efforts prior to expensive discovery.

C. *Increasing Certainty in Public Enforcement Actions*

In the public context, reducing uncertainty is more difficult. Public enforcement authority always entails some degree of government discretion. Courts can, however, increase certainty by raising the costs of public enforcement actions *for the government*. Specifically, courts could interpret statutes in ways that either prohibit domain name seizures or at least require higher showings by the government. Courts could also effectively impose notice requirements prior to domain name seizures. In criminal prosecution, courts could clarify that criminal liability does not extend to activities (such as mere linking) traditionally governed by civil secondary liability. They could also clarify that certain provisions—such as "willfulness"—require a high showing to survive early dispositive motions. In this way, my proposals strike an appropriate balance between protecting platforms and ensuring that government officials retain sufficient authority to pursue the more problematic infringers.

1. Reforming Domain Name Seizures

The cloud of uncertainty surrounding domain name seizures stems from the government's ability to act without prior notice or adversarial hearings. These actions not only chill investment and legitimate activity, they potentially create a prior restraint that violates the First Amendment. There are, however, ways to interpret the forfeiture statutes that would at least partially remedy these problems.

One possibility is to hold that domain names are not "property" under § 2323(a), which would effectively prohibit domain name seizures

370 17 U.S.C. § 512(a)–(d) (2012); UMG Recordings, Inc. v. Veoh Networks, Inc., CV 07-5744, 2009 WL 334022 (C.D. Cal. Feb. 2, 2009).

under this statute.[371] While this interpretation is admittedly broad, the legislative history offers some support. In particular, the *lack* of discussion about domain names seizures supports interpreting "property" to mean tangible items. In addition, the statute replaced section 509 of the Copyright Act, which was phrased in terms of physical items.[372] The practical effect of this interpretation would be to force Congress to consider domain name seizures in a more open and transparent process. In addition, it would allow courts to avoid the more difficult constitutional questions surrounding prior restraint.

A second possibility is to construe § 2323 as requiring a reasonable belief that the *facilitator* is committing criminal infringement. Under this reading, the government must establish direct infringement by the owner of the facilitating property, rather than merely the existence of third-party criminal infringement. Further, courts should be skeptical of accomplice liability claims that effectively criminalize civil secondary liability. In the case of § 2323(a), courts can easily dismiss such charges because the statute does not incorporate the federal aiding and abetting statute in its list of underlying criminal activities that justify seizures.[373]

A final possibility would not necessarily prevent seizures, but would instead allow sites to reclaim domain names quickly. § 2323 forfeitures are governed by other procedural requirements including 18 U.S.C. § 983(f), which allows parties to petition courts for the "immediate release of seized property."[374] To obtain release, parties must establish—among other things—that the continuing seizure will cause "substantial hardship," and that there is little risk that evidence will be lost or destroyed.[375] Courts, however, could interpret § 983(f) to hold that domain names presumptively satisfy these criteria. Unlike tangible property, domain names are in little danger of being lost or concealed, particularly given that they are controlled by United States registries. Further, because a domain name is so central to a website's operations, seizures necessarily create a substantial hardship. Again, while these interpretations of § 983(f) would not technically prevent seizures, they could discourage them if site operators could immediately and reliably obtain their release.

---

371 18 U.S.C. § 2323(a)(1) (2012).

372 17 U.S.C. § 509, *repealed by* PRO-IP Act of 2008, Pub. L. No. 110-403, § 201, 122 Stat. 4256, 4260; Eric Goldman, *Catching Up on 4 Months of Online Copyright Cases—Myxer, Hotfile, Megaupload, Flava Works, Zediva, Blue Nile, Perfect 10, Rojadirecta*, TECH. & MKT'G LAW BLOG (Aug. 12, 2011), http://blog.ericgoldman.org/archives/2011/08/catching_up_on.htm ("The applicable statute was designed to govern physical chattel, not virtual printing presses.").

373 *Puerto 80* Motion to Dismiss, *supra* note 258, at 8–9.

374 18 U.S.C. § 983(f).

375 *Id.* § 983(f)(1)(C)–(D).

2. Reforming Criminal Prosecutions

The uncertainty that expanded criminal prosecution creates is perhaps the most difficult to address. Because prosecution necessarily entails a degree of discretion, the uncertainty cannot be completely eliminated. Courts can, however, force the government to internalize more of the costs of prosecution through certain statutory interpretations. One possibility is to clarify that "willfulness" requires evidence of subjective specific intent. In particular, courts should be skeptical of claims that normal business practices—particularly efforts to prevent infringement—can constitute intent. Indeed, one of the more troubling aspects of the Megaupload indictment is the government's attempt to cite prevention efforts as evidence of subjective intent.[376] More broadly, courts should be wary of attempts to criminalize civil secondary liability. In particular, they should respect well-established precedent that limits the scope of criminal liability. Courts should, for instance, reject efforts to transform mere linking into grounds for criminal liability.

In general, however, the problem of expanded criminal prosecution is likely a political one. Indeed, one critique of the recent prosecutions is that the government is acting as a proxy for private interests.[377] News reports have confirmed that the music and film industry played important roles in the Megaupload prosecution and the Dajaz1 domain name seizure.[378] In this sense, criminal prosecution is an example of agency capture. Accordingly, the more that the public and policymakers object to these efforts, the higher the political costs of such actions become.

3. Procedural Protections

One final way to raise the government's costs in bringing public enforcement actions is to increase due process protections. The presence of notice and adversarial hearings would substantially reduce one of the most important sources of uncertainty—the possibility that one's website could "disappear" without prior warning. For instance, congressional critics of SOPA and PIPA introduced an alternative

---

376 *See supra* notes 296–297 and accompanying text.

377 Goldman, *supra* note 290 ("[T]he government's prosecution of Megaupload demonstrates the implications of the government acting as a proxy for private commercial interests.").

378 Sisario, *supra* note 65; Greg Sandoval, *Critics Say Feds, RIAA Too Closely Linked in Music Site Seizure*, CNET, (May 4, 2012), http://news.cnet.com/8301-1023_3-57428362-93/critics-say-feds-riaa-too-closely-linked-in-music-site-seizure.

measure to combat foreign infringing sites called the OPEN Act.[379] One key distinction is that it creates a new adversarial process overseen by the International Trade Commission that contains more due process protections than SOPA and PIPA did.[380] The larger principle, however, is more important than any specific legislation. Any future law should ultimately incorporate procedural protections that not only deter frivolous enforcement actions, but that ensure the government will be better informed prior to initiating enforcement actions.

Courts could also require procedural protections by finding that public enforcements actions such as domain name seizures create prior restraints under the First Amendment. Such a finding would require procedural protections independent of what the federal forfeiture statutes may require. Because of space constraints, the First Amendment analysis is beyond the scope of this Article.

CONCLUSION

Internet platforms are unique in terms of their ability to generate low-cost expression and innovation. The same factors that generate these benefits, however, also make them susceptible to expensive copyright litigation—particularly when the legal doctrine is sufficiently broad and uncertain. While courts and policymakers must respect the rights of content owners, these rights can be respected in ways that do not threaten the existence—and future evolution—of Internet platforms. Indeed, the evolution of technologies such as the VCR and YouTube illustrates how new technologies can—assuming they survive—ultimately benefit content owners. As one writer put it, "yesterday's Napster is today's iTunes."[381] In this respect, clarifying the law to protect Internet platforms will likely benefit all parties over time.

379 Nate Anderson, *Censorship Foes Roll Out Antipiracy Plan*, ARS TECHNICA (Dec. 8, 2011), http://arstechnica.com/tech-policy/2011/12/censorship-foes-roll-out-antipiracy-plan-say-stop-butchering-the-internet.

380 *Id.*

381 Peter Nowak, *Canada's Telecom Situation Reaches Boiling Point*, WORDSBYNOWAK (Feb. 2, 2011), http://wordsbynowak.com/2011/02/02/canadas-telecom-situation-reaches-boiling-point.