Uncertainty as Enforcement Mechanism: The New Expansion of Secondary Copyright Liability to Internet Platforms

John Blevins
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. Critically, copyright owners and the government do not necessarily need to prevail in these actions. Instead, the proceedings can be effective so long as they impose sufficient costs upon Internet platforms. In this respect, prevailing is less important than obtaining statutory and doctrinal constructions that are expensive for platforms to litigate. In this article, I argue that these enforcement actions can be understood as efforts to institutionalize legal uncertainty within secondary liability doctrines. This uncertainty, once established, effectively expands secondary copyright liability by raising the costs of private and public enforcement actions and by shifting the burden of enforcement to Internet platforms. Below, I describe and critique this expansion, and then propose measures to strengthen and clarify Internet platforms’ defenses.

* Associate Professor of Law, Loyola University New Orleans College of Law. I would like to thank Eric Goldman, James Grimmelmann, Stacey Lantagne, Edward Lee, and Elizabeth Townsend-Gard for being willing to review drafts. I also thank participants of the faculty workshop at Loyola University New Orleans.
INTRODUCTION ................................................................................................................................. 3

I. THE BENEFITS OF UNCERTAINTY FOR COPYRIGHT OWNERS ............................................... 6
A. The Legal Efforts Against Internet Platforms ................................................................. 6
B. The Benefits of Uncertainty ...................................................................................... 8
   1. The Benefits for Private Litigation ................................................................. 8
   2. The Benefits for Public Enforcement .......................................................... 12

II. INSTITUTIONALIZING UNCERTAINTY IN PRIVATE LITIGATION ..................................... 13
A. Section 512 Safe Harbor—Blurring the Bright Lines ........................................ 14
   1. “Red Flag” Knowledge .............................................................................. 17
   2. Adequate Notice ........................................................................................ 20
   3. Service Providers and Protected Services .............................................. 22
   4. Reasonable Removal Policy .................................................................. 23
   5. Right to Control and Financial Benefit ................................................. 24
B. The Decline of the Sony Defense ...................................................................... 28
C. Other Efforts to Increase Uncertainty .............................................................. 30
   1. The Rise of Inducement Liability .......................................................... 30
   2. Expanding Direct Infringement .............................................................. 32
   3. Suing Investors ....................................................................................... 34

III. INSTITUTIONALIZING UNCERTAINTY IN PUBLIC ENFORCEMENT ACTIONS ....................... 35
A. Domain Name Seizures ...................................................................................... 35
   1. Technical and Legal Overview ................................................................ 35
   2. Uncertainty Through New Legislation .................................................. 37
   3. Uncertainty Through New Statutory Interpretations .............................. 39
B. SOPA and PIPA ............................................................................................... 43
C. Criminal Prosecution ....................................................................................... 46

IV. NORMATIVE ANALYSIS OF EXPANDED UNCERTAINTY ..................................................... 49
A. Policy Tradeoffs of Secondary Liability .......................................................... 50
B. Secondary Liability and Internet Platforms .................................................. 51

V. HOW TO BETTER PROTECT INTERNET PLATFORMS ........................................................ 55
A. Increasing Certainty in Private Enforcement Actions ...................................... 56
   1. Improving the DMCA Safe Harbor ......................................................... 56
   2. Improving the Sony Defense ................................................................. 60
B. Increasing Certainty in Public Enforcement Actions ...................................... 62
   1. Reforming Domain Name Seizures ......................................................... 62
   2. Reforming Criminal Prosecutions ......................................................... 64
   3. Procedural Protections ......................................................................... 64
INTRODUCTION

In 2011, a video-sharing site called Veoh won a big victory in the Ninth Circuit. 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. Major record labels ultimately sued Veoh for secondary copyright liability, but Veoh prevailed at both the district court and in the Ninth Circuit. 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.

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

These enforcement proceedings share a common theme. In both, the parties enforcing copyrights succeeded in altering behavior without prevailing in the case. Indeed, the Veoh litigation helped bankrupt the company even though federal courts ultimately ruled that the site was

---

1 UMG Recordings v. Shelter Capital Partners, 667 F.3d 1022, 1026 (9th Cir. 2011).
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”).
6 See infra Part III.C.
The lesson is that copyright enforcement against Internet platforms can succeed merely by increasing the costs of enforcement proceedings. The more expensive that enforcement proceedings become, the more effectively they can be leveraged as enforcement mechanisms.

In this article, I explore the role that uncertainty plays as a copyright enforcement mechanism against Internet platforms. Specifically, I argue that recent enforcement proceedings—both private and public—can be understood as efforts to institutionalize legal uncertainty within secondary liability doctrines. This uncertainty, once established, effectively expands the scope of secondary copyright liability and raises the costs of enforcement proceedings in ways that disproportionately harm Internet platforms. The risk of higher costs not only provides copyright enforcers with greater leverage, it creates incentives for Internet platforms to become co-enforcers of third-party copyrights. In this respect, uncertainty allows content owners and the government to “outsource” enforcement costs to Internet platforms.

In the private context, I argue that recent secondary liability litigation can be understood as a dispute between rules and standards. I examine these disputes by focusing on the potential defenses platforms have to secondary liability claims—particularly the DMCA safe harbor and Sony defenses. In these cases, Internet platforms prefer statutory (or doctrinal) interpretations that create clear bright-line rules with low administrative costs. Copyright owners, by contrast, prefer statutory interpretations that impose uncertain fact-intensive standards that require expensive discovery and that cannot be resolved by early dispositive motions. In short, platforms prefer interpretations that reduce litigation costs, while content owners prefer those that increase them.

In the public context, I argue that the government is expanding secondary liability by increasing uncertainty through both 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. In all of these contexts, the government is pursuing doctrines and interpretations that would blur and expand the boundaries of its enforcement authority. This expansion, in turn, provides

---

8 See infra Part I.A.
9 Technically, and as I explain in Part III, criminal secondary liability 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.
10 See infra Part I.
11 See infra Part II.A-B.
12 See infra Part III.
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. 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.

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, it 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, viewing these contexts collectively helps inform the policy analysis in any one context. For instance, the costs of the expansive statutory interpretations in the domain name seizure context urges skepticism of similar language in the SOPA and PIPA bills. Finally, my framework also provides a practical guide to courts presiding over secondary liability proceedings against Internet platforms.

Part I summarizes the private and public enforcement actions that Internet platforms 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, and then justifies these choices.

---

13 See infra Part IV.A.
14 See infra Part IV.B.
15 See infra Part III.A-B.
16 See infra Part V.
I. THE BENEFITS OF UNCERTAINTY FOR COPYRIGHT OWNERS

This section provides an overview of the recent copyright enforcement actions against Internet platforms. I begin by describing 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.\(^\text{17}\) The most common targets are platforms that support “user generated content” (UGC)—which is content supplied independently by third-party users.\(^\text{18}\) 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.\(^\text{19}\) Other common targets are “information location” sites such as search engines that help users locate—and link to—third-party content.\(^\text{20}\)

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.\(^\text{21}\) 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.22

A second category of targeted platform services is “aggregator” sites that provide links to third-party infringing content.23 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.24 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.25

A third category of targeted platform services is video and photo sharing sites.26 These sites allow users to upload and share their files. The most popular video-sharing platform is YouTube, but the category also includes sites such as Veoh, Vimeo, Facebook, and Funnyordie. Photo-sharing sites includes sites like Instagram, Pinterest, and Photobucket.

---

22 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, 731-33 (2012).
23 Aggregators have recently faced a wave of public enforcement actions such as domain names 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 & III.C. Private litigation against aggregators is not new, but has targeted sites like Google, Amazon, and eBay. See, e.g., Perfect 10 v. Amazon.com, 508 F.3d 1146 (9th Cir. 2007); Corbis Corp. v. Amazon.com, 351 F. Supp. 2d 1090 (W.D. Wash. 2004); Hendrickson v. Amazon.Com, 298 F. Supp. 2d 914 (C.D. Cal. 2003); Hendrickson v. eBay, 165 F. Supp. 2d 1082 (C.D. Cal. 2001).
24 Rojadirecta linked to sporting event streams. See infra Part III.A.
25 The Megaupload indictment alleges that the company conspired with third-party aggregators. Megaupload Indictment, supra note 21, at ¶¶11-14.
26 Examples of private litigation against these sites include Viacom Int’l v. YouTube, 676 F.3d 19 (2d Cir. 2012); Wolk v. Kodak Imaging Network, 840 F. Supp. 2d 724 (S.D.N.Y. 2012) (Photobucket); UMG Recordings v. Shelter Capital Partners, 667 F.3d 1022 (9th Cir. 2011) (Veoh).
A fourth category is peer-to-peer file sharing services, which have featured prominently in copyright litigation for over a decade. These services provide software that allows users to locate and download files on individuals’ computers in the absence of centralized architecture. 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.

The various Internet platforms described above currently face both private and public copyright enforcement proceedings. By private 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. The substance of their claims is that platforms should be liable for facilitating the infringement of others. 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.

B. The Benefits of Uncertainty

This section explains copyright enforcers’ motives for preferring uncertain legal standards in these various proceedings. Specifically, I argue that uncertainty raises the costs of enforcement proceedings in ways that disproportionately affect Internet platforms.

1. The Benefits for Private Litigation

---

27 The three leading cases regarding peer-to-peer networks are Metro-Goldwyn-Mayer Studios v. Grokster, 545 U.S. 913 (2005), In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003), and A&M Records, Inc. v. Napster, 239 F.3d 1004 (9th Cir. 2001).
31 Lemley & Reese, supra note 17, at 1346-47.
In general, legal standards are more costly to enforce than bright-line rules in private litigation. 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 litigation effectively costs smaller parties more.

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. 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. 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.”

The bankruptcy of the startup Veoh illustrates this dynamic. Veoh was launched in 2005 as a video-sharing service. Within a year of its

---

34 Lisa Bernstein, Social Norms and Default Rules Analysis, 3 S. CAL. INTERDISC. L.J. 59, 90 (1993) (“The ability to threaten to impose high litigation costs will improve the bargaining position of the party with superior resources.”).
35 For instance, Universal Music is suing Veoh and Grooveshark. Shelter Capital Partners, 667 F.3d at 1026 (Veoh); Grooveshark Complaint, supra note 21, at ¶3-4. Capitol Records is suing Redigi. Redigi Complaint, supra note 21, at ¶5-6. Several music labels are collectively suing MP3Tunes and Limewire. MP3Tunes, 821 F. Supp. 2d at 633; Lime Group, 715 F. Supp. 2d at 492. Various movie studios are suing Isohunt and other related sites. Fung, 2009 WL 6355911 at *1 n.1. 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, 515 (S.D.N.Y. 2010).
37 Id. (citing Veoh as an example).
38 Jefferson Graham, Veoh Aims to be One-Stop Shop for Net TV Viewers, USA TODAY, Feb. 27, 2008, at 8B. Veoh also had a peer-to-peer client application. Id.
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. 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. Veoh’s ambitions also evolved as the company sought to “democratize broadcasting” by becoming the world’s first virtual cable network.

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

[The 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

---

43 *UMG*, 667 F.3d at 1026; *UMG*, 665 F. Supp. 2d at 1100-01.
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.  

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

The Viacom-YouTube litigation provides another illustration of this dynamic. In 2006, Viacom sued YouTube for more than one billion dollars. Like Veoh, YouTube has been largely successful at both the district and appellate court level, though its legal costs are estimated to be over $100 million thus far. 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.”

Most UGC companies, however, lack access to such resources when faced with copyright litigation that poses an existential threat.

The more general principle is that Internet platforms are particularly vulnerable to expensive copyright litigation. Accordingly, as legal standards become more uncertain and thus more expensive, private copyright litigation becomes progressively more threatening. These risks are compounded by copyright law’s notoriously uncertain range of

47 Masnick, supra note 4.
monetary damages. 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 standards that would effectively require Internet platforms to affirmatively police their own sites for copyright infringement.

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. 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. 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. Some sites disabled sharing altogether, while others vowed to terminate

---

52 See, e.g., Alan E. Garfield, Calibrating Copyright Statutory Damages to Promote Speech, 38 FLA. ST. U. L. REV. 1, 6-7 (2010).
53 See e.g., In re, 586 F. Supp. 2d at 1154 (“[Plaintiff’s] not-so-subtle suggestion is that, if Veoh cannot prevent infringement from ever occurring, then it should not be allowed to exist.”). See also infra at 26.
54 Dan Markel, How Should Punitive Damages Work?, 157 U. PA. L. REV. 1383, 1484 (2009) (observing that “a civil sanction . . . is qualitatively different from criminal penalties because such damages entail no resulting conviction [and] less of a stigma”).
any subscriber that a content owner suspects is infringing. 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. As it turned out, artists and record labels had leaked the pre-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. 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 section argues that the legal disputes in private litigation can be understood as a conflict of rules versus standards. This framing helps clarify case law, and illustrates how copyright owners are attempting to institutionalize uncertain legal standards within the doctrines most relevant to Internet platforms—specifically, the Section 512 safe harbor, the Sony doctrine, and other common law secondary liability standards.

---

58 Application and Affidavit for Seizure Warrant, No. 10-2822M, at ¶80 (C.D. Cal. filed on Nov. 17, 2010) (Dajaz1 Seizure Warrant).
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 Section 512 of the Digital Millennium Copyright Act (DMCA). Enacted in 1998, Section 512 was a compromise between major content owners and technology companies. Content owners feared that the Internet would enable an unprecedented wave of infringement, while technology companies feared being sued for providing general-purpose services such as data transmission and storage. Private parties eventually hammered out a compromise, and Congress incorporated it into the DMCA.

Section 512 is a complex statute, but the basic idea is simple. Defendants can invoke Section 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. A central dispute, therefore, in these cases is whether defendants who invoke Section 512 comply with the various statutory prerequisites.

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...
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 Section 512(c), while aggregation sites potentially fall under 512(d). Both sections, however, are substantively similar.

Assuming a party is a service provider under 512(c) or 512(d), it must also comply with a miscellaneous set of provisions designed to ensure that it 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. 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; (2) the defendant must not enjoy a direct financial benefit from infringing activity that it has the right and ability to control; (3) the defendant must have established adequate “notice and takedown” procedures and complied with them; and (4) the defendant must have instituted and implemented adequate policies to remove repeat infringers.

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. If the notice is defective (e.g., too broad, lacking in detail), it cannot create the “knowledge” of infringement that would trigger takedown

---

66 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 v. YouTube, 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.”).
68 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)[.]”).
70 17 U.S.C. §512(c)(1)(A); §512(d)(1).
71 17 U.S.C. §512(c)(1)(B); §512(d)(2).
72 17 U.S.C. §512(c)(2).
73 17 U.S.C. §512(i).
74 17 U.S.C. §512(c)(3)(A); §512(d)(3).
obligations. Section 512 further protects technology companies by explicitly stating that they have no affirmative duty to monitor their sites for infringement.

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. And because Section 512 imposes so many prerequisites, it creates incentives to litigate multiple statutory provisions.

In the sections below, I examine the most contested statutory provisions of Section 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 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.

Viewing these disputes through this lens yields several benefits. First, it helps clarify trends in the Section 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 Section 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 Section 512 includes so many statutory requirements, the plaintiffs need only establish uncertainty in one provision to effectively neutralize the safe harbor.

---

75 17 U.S.C. §512(c)(3)(B)(i). In some instances, however, a partially compliant notice can create knowledge unless the service providers makes efforts to obtain a fully compliant one. 17 U.S.C. §512(C)(3)(B)(ii).
76 17 U.S.C. §512(m)(1) (providing that DMCA immunity not conditioned on “a service provider monitoring its service or affirmatively seeking facts indicating infringing activity”).
short, a bad result with a good interpretation is better than a good result with a bad interpretation.

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.\(^{79}\) These two levels of knowledge are distinct under the statute.\(^{80}\) Actual knowledge is a purely subjective standard, while apparent knowledge—also called “red flag” knowledge—incorporates subjective and objective standards.\(^{81}\) Red flag knowledge is created by awareness of “facts or circumstances from which infringing activity is apparent.” \(^{82}\) As the Second Circuit has explained, the service provider must be “subjectively aware of facts that would have made the specific infringement ‘objectively’ obvious to a reasonable person.” \(^{83}\)

Understandably, copyright owners and Internet platforms disagree on how to construe these provisions. Internet platforms seek to narrow 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.\(^{84}\) In practice, this interpretation implies that knowledge is triggered only when copyright owners specifically identify infringement (generally by listing URLs) in a DMCA notice.\(^{85}\) 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

\(^{79}\) 17 U.S.C. §512(c)(1)(A); §512(d)(1).
\(^{81}\) S. Rep. 105-190, at 44 (1998) (“The ‘red flag’ test has both a subjective and an objective element.”) (Senate DMCA Report).
\(^{82}\) 17 U.S.C. §512(c)(1)(A)(ii); §512(d)(1)(B).
\(^{83}\) YouTube, 676 F.3d at 31.
\(^{85}\) These arguments are documented in the next section regarding adequate notice. See infra Part II.A.2.
infringement, as opposed to knowledge of specific instances of infringement.\textsuperscript{86} They also argue that apparent knowledge encompasses “willful blindness” by platforms.\textsuperscript{87} The key distinction, however, is these interpretations imply that facts \textit{external} to the DMCA notice can give rise to knowledge.\textsuperscript{88} 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 uncertain about when knowledge exists, they will be more likely to monitor their sites aggressively and remove material liberally.\textsuperscript{89}

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 \textit{Aimster}, the district court essentially equated the red flag provisions with the knowledge requirements of contributory liability (which are notoriously vague).\textsuperscript{90}

As the decade progressed—and as defendants expanded beyond peer-to-peer companies—courts narrowed their interpretations. In the 2007 case \textit{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

\textsuperscript{86} \textit{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”); \textit{UMG}, 667 F.3d at 1036-37 (noting UMG’s argument that “general knowledge” is sufficient); \textit{Corbis}, 351 F. Supp. 2d at 1108. \textit{See also} Brief of Amici Curiae Broadcast Music, Inc. (BMI), et al., Viacom Int’l v. YouTube at 22-23, No. 10-3270 (2d Cir. Dec. 10, 2010) (“The DMCA . . . leaves the “facts and circumstances” constituting “knowledge or awareness” to be decided on a case by case basis.”) (\textit{BMI YouTube Brief}).

\textsuperscript{87} \textit{See}, e.g., \textit{Brief of Motion Picture Assoc. of America} at 22-25, Viacom Int’l v. YouTube at 29-30, No. 10-3270 (2d Cir. Mar. 31, 2011) (contending the specific knowledge standard “encourages willful blindness”) (\textit{MPAA YouTube Brief}).

\textsuperscript{88} \textit{See infra} at Part II.A.2.

\textsuperscript{89} \textit{See}, e.g., \textit{Brief for Amici Curiae [BMI and ASCAP]}, at 6-7, \textit{UMG Recordings v. Veoh Networks}, No. 09-56777 (9th Cir. Apr. 27, 2010) (arguing that 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”) (\textit{BMI Veoh Brief}).

\textsuperscript{90} In re \textit{Aimster Copyright Litig.}, 252 F. Supp. 2d 634, 661 (N.D. Ill. 2002) (holding that constructive knowledge under common law contributory liability also nullifies DMCA defense). \textit{See also} \textit{Arista Records, Inc. v. Mp3Board, Inc.}, 00 Civ. 4660 (SHS), 2002 WL 1997918 at *10 (S.D.N.Y. Aug. 29, 2002). On the vagueness of contributory liability, \textit{see infra} note 159.
sites. 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. 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. 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. First, the court held that “willful blindness” could establish apparent knowledge and remanded the case on that basis. 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. 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. 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

---

91 Perfect 10 v. CCBill, 488 F.3d 1102, 1113-15 (9th Cir. 2007).
93 CCBill, 488 F.3d at 1114-15 (“We do not place the burden of determining [legality] on a service provider.”). See also YouTube, 676 F.3d at 32 (quoting CCBill); UMG, 667 F.3d at 1035-38 (same); Io, 586 F. Supp. 2d at 1149 (same).
95 YouTube, 676 F.3d at 34-35.
96 Id. at 32-34.
97 See generally Goldman, supra note 77.
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.” The “identification” must include “information reasonably sufficient” to allow the service provider “to locate the material.” Adequate notice creates both actual and apparent knowledge, which in turn triggers takedown obligations. Inadequate notices, by contrast, do not create such knowledge, and thus cannot—by themselves—trigger takedown obligations.

The central dispute in this context turns on how specific a DMCA notice must be. Unsurprisingly, Internet platforms favor bright-line interpretations that 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. For platforms, the most important point is that a notice cannot create amorphous obligations to remove content not specifically listed in the notice.

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. This provision, they argue, expressly contemplates infringing activity not specifically listed in a

---

100 17 U.S.C. §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. 17 U.S.C. §512(c)(3)(B)(ii).
101 See, e.g., Brief for Defendants-Appellees at 29-30, Viacom Int’l v. YouTube, No. 10-3270 (2d. Cir. March 31, 2011); (arguing that 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 omitted).
takedown notice.\textsuperscript{104} 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.\textsuperscript{105} The shift began in 2003, when a district court ruled that notices must point to current infringing activity rather than potential future infringement.\textsuperscript{106} The Ninth Circuit further narrowed 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.”\textsuperscript{107} 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.\textsuperscript{108} 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.\textsuperscript{109} In UMG, the Ninth Circuit held that merely identifying a list of artists was insufficient.\textsuperscript{110} 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.\textsuperscript{111} Such a requirement, the court held, “would eviscerate the required specificity of notice,” and would violate Section 512(m), which expressly relieves defendants of the duty to affirmatively monitor their sites.\textsuperscript{112} 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

\textsuperscript{104} BMI Veoh Brief, supra note 89, at 9-11 (noting that narrow construction would “eviscerate the representative list provision”). See also YouTube, 718 F. Supp. 2d at 528-29.

\textsuperscript{105} YouTube, 676 F.3d at 30-32; UMG, 667 F.3d at 1036-38; CCBill, 488 F.3d at 1111-13; Wolk 840 F. Supp. 2d at 746-47; MP3Tunes, 821 F. Supp. 2d at 642-43.


\textsuperscript{107} CCBill, 488 F.3d at 1111-13.

\textsuperscript{108} Id. at 1112.

\textsuperscript{109} MP3Tunes, 821 F. Supp. 2d at 642.

\textsuperscript{110} UMG, 667 F.3d at 1039.

\textsuperscript{111} YouTube, 718 F. Supp. 2d at 528-29.

\textsuperscript{112} Id.
material.” This language, they conclude, implies a formal requirement of specificity.\(^{113}\)

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),\(^{114}\) and the infringement must arise from a specified protected service.\(^{115}\) The litigation relevant to this article focuses on services protected by Section 512(c) (data storage by users) and 512(d) (information location). The precise language of 512(c) shields platforms from liability for infringement “by reason of storage at the direction of a user.”\(^{116}\)

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”\(^{117}\) and covers a “broad variety of Internet activities.”\(^{118}\) Courts have also adopted broad interpretations of the protected services listed in Section 512(c)-(d).\(^{119}\) In particular, courts have consistently affirmed that the DMCA protects not just storage, but other related features that are “attributable to storage.”\(^{120}\) 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

\(^{113}\) Id.; UMG, 665 F. Supp. 2d at 1110.

\(^{114}\) This article focuses primarily on the second type of “service provider” under 17 U.S.C. § 512(k)(1)(B).

\(^{115}\) 17 U.S.C. § 512(a)-(d).

\(^{116}\) 17 U.S.C. § 512(c)(1).

\(^{117}\) Aimster, 252 F. Supp. 2d at 658 (“[W]e have trouble imagining the existence of an online service that would not fall under the definitions[,]”); Perfect 10 v. Cybernet Ventures, 213 F. Supp. 2d 1146, 1175 (C.D. Cal. 2002) (“Section 512(k)(1)(B)’s definition has been interpreted broadly.”). Hendrickson v. eBay., 165 F. Supp. 2d 1082, 1088 (C.D. Cal. 2001).

\(^{118}\) Corbis, 351 F. Supp. 2d at 1099-1100.


\(^{120}\) UMG, 665 F. Supp. 2d at 1089. See also YouTube, 676 F.3d at 38-40; UMG, 667 F.3d at 1031-35.
services that platforms provide. The crux of their strategy is to identify additional services ancillary to storage that are not technically “storage.” In the Veoh litigations, content owners argued that various software functions associated with video uploads fall outside 512(c)’s protected services. 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. The plaintiffs in YouTube raised similar arguments.

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 fact issues exist regarding any single ancillary software function, that holding can be used to extend litigation and obtain discovery in future cases.

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.” 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 Section 512(i) and its legislative history were “less than models of clarity.” And courts in the early DMCA

---

121 See, e.g., Memorandum of Law in Support of Viacom’s Motion for Partial Summary Judgment at 61, Viacom Int’l v. YouTube, No. 10-3270 (2d. Cir. March 18, 2010) (“Defendants fall outside the DMCA [because] their infringement does not result from providing the specified core Internet functions covered by the defense.”).  
123 UMG, 667 F.3d at 1031-32; Jo, 586 F. Supp. 2d at 1146-48.  
124 Id.  
125 YouTube, 676 F.3d at 38-39.  
127 Cybernet Ventures, 213 F. Supp. 2d at 1176.
cases often ruled for copyright owners by finding factual issues regarding platforms’ removal policies.\textsuperscript{128}

More recent cases, however, demonstrate a clear trend toward a rule-like interpretation of these provisions that lowers administrative costs. The Ninth Circuit’s 2007 opinion in \textit{CCBill} illustrates this interpretative shift. After noting that the statute does not define “reasonably implement,” it announced a new \textit{element-based} definition.\textsuperscript{129} The court held that parties “implement” 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.”\textsuperscript{130} It also clarified that “reasonableness” does not require service providers to “affirmatively police” its users.\textsuperscript{131} Together, these definitions significantly clarify and formalize Section 512(i)’s requirements. And later courts have relied on this clarification in ruling for platforms.\textsuperscript{132}

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.”\textsuperscript{133} 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).\textsuperscript{134} 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.\textsuperscript{135}

\textsuperscript{128} \textit{Id.} at 1175-79. \textit{See also} \textit{Aimster}, 252 F.Supp.2d at 658-59; \textit{Loopnet}, 164 F. Supp. 2d at 703-04.
\textsuperscript{129} \textit{CCBill}, 488 F.3d at 1109-10.
\textsuperscript{130} \textit{Id.}
\textsuperscript{131} \textit{Id.} at 1111.
\textsuperscript{133} 17 U.S.C. §512(c)(1)(B); §512(d)(2).
\textsuperscript{134} 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 Pub’g v. Columbia Artist Mgmt., 443 F.2d 1159, 1162 (2d Cir.1971)). \textit{But see} Lee, \textit{supra} note 67, at 240-42 (arguing that text differs from common law standard).
Copyright owners, unsurprisingly, argue that the two doctrines are coextensive.\footnote{UMG Brief, supra note 122, at 67-69 (arguing that DMCA provisions “track the elements of vicarious liability under long-standing copyright principles”); BMI YouTube Brief, supra note 86, at 26.} 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.”\footnote{Id.; CCBill, 488 F.3d at 1117-18.} Because the DMCA’s language did have settled meaning, courts should therefore infer that the requirement is coextensive with vicarious liability. The implication is that Section 512 directly incorporates the common law vicarious liability standards.

This interpretation not only prevents platforms from invoking the safe harbor for vicarious liability claims, it also is 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).\footnote{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).} Through time, however, the doctrine expanded well beyond its agency law foundations.\footnote{Grossman, supra note 138, at 370-71; Sverker K. Högberg, The Search for Intent-Based Doctrines of Secondary Liability in Copyright Law, 106 COLUM. L. REV. 909, 92-30 (2006); Lee, supra note 67, at 236-37; Lemley and Reese, supra note 17, at 1366-68.} 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.\footnote{Helman & Parchomovsky, supra note 36, 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 139, at 939-33; Lemley and Reese, supra note 17, at 1367-68.} Thus, by incorporating the common law standard into Section 512, copyright owners benefit from vague and fact-intensive standards that are difficult to resolve in dispositive motions—and that are wholly 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].”\footnote{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).} The court

---

\textbf{Lemley, Rationalizing Internet Safe Harbors, 6 J. TELECOMM. & HIGH TECH. L. 101, 113-14 (2007).}
\textbf{136} UMG Brief, supra note 122, at 67-69 (arguing that DMCA provisions “track the elements of vicarious liability under long-standing copyright principles”); BMI YouTube Brief, supra note 86, at 26.
\textbf{137} Id.; CCBill, 488 F.3d at 1117-18.
\textbf{140} Helman & Parchomovsky, supra note 36, 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 139, at 939-33; Lemley and Reese, supra note 17, at 1367-68.
granted some requests, and denied others. 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 the ability to control infringement.” The plaintiffs in the Io litigation raised similar arguments in discovery.

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. Specifically, they argue that copyright owners’ interpretations would effectively nullify the safe harbor and impose affirmative monitoring costs upon them. 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.

Courts have been inconsistent on these questions, to put it mildly. 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

---

142 Id. at 265.
143 Id. at 262-63 (emphasis added).
145 See, e.g., Veoh Brief, supra note 84, at 50-53 (arguing that UMG interpretation “negates the purpose of the DMCA”).
147 MPAA YouTube Brief, supra note 87, at 6.
148 For cases interpreting the DMCA similarly to the common law standard, see CCBill, 488 F.3d at 1117-18; Io, 586 F. Supp. 2d at 1150. For cases interpreting them differently, see YouTube, 676 F.3d at 36; UMG, 667 F.3d at 1043-45.
requirement. 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 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.” 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 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 control requires “something more” than simply the ability to remove content or terminate users. It would be illogical if an activity contemplated by the safe harbor (i.e., removal of content) simultaneously precluded its use. 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 atextual. The court did not, however, provide an alternative interpretation—it merely disagreed with both parties’ interpretations and remanded. 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

149 UMG, 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.”); YouTube, 718 F. Supp. 2d at 527.
150 UMG, 667 F.3d at 1043 (emphasis added).
151 See, e.g., YouTube, 676 F.3d at 37; UMG, 667 F.3d at 1043; Wolk 840 F. Supp. 2d at 747-48, Io, 586 F. Supp. 2d at 1151; Corbis, 351 F. Supp. 2d at 1109-10.
152 Io, 586 F. Supp. 2d at 1151 (stating that “a contrary holding would render the DMCA internally inconsistent”). See also YouTube, 676 F.3d at 36-38.
153 YouTube, 676 F.3d at 36.
154 Id. at 38.
reasons, Eric Goldman has predicted that plaintiffs will forum shop cases in the Second Circuit, where the doctrine is far more unsettled.\textsuperscript{155}

B. The Decline of the \textit{Sony} Defense

Assuming platforms are ineligible for the safe harbor, courts must still determine whether they meet the requirements for secondary liability. The three secondary liability doctrines—contributory liability, vicarious liability, and inducement liability—are not found in the Copyright Act, but are instead judicial creations.\textsuperscript{156} The common law doctrines of contributory and vicarious liability have a long history, and the Copyright Act of 1976 implicitly recognizes them even though it does not define them.\textsuperscript{157} Inducement liability is more recent, and was created by the Supreme Court in the 2005 \textit{Grokster} case.\textsuperscript{158}

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.\textsuperscript{159} 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 \textit{Sony} defense.

The basics of \textit{Sony} are well known. In 1984, the Supreme Court saved the VCR from copyright litigation.\textsuperscript{160} 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 \textit{Sony}, then, was whether VCR manufacturers could be secondarily

\textsuperscript{155} Goldman, \textit{supra} note 77 (“I expect future 512 cases will be brought in the Second Circuit, not the Ninth Circuit.”).
\textsuperscript{159} Mark Bartholomew & Patrick F. McArdle, \textit{Causing Infringement}, 64 \textit{VAND. L. REV.} 675, 678-79 (2011); Giblin, \textit{supra} note 135; Högberg, \textit{supra} note 139, at 914.
liable for the infringement of their users. The Supreme Court rejected this argument, holding that devices “capable of substantial noninfringing uses” cannot be liable for secondary infringement.

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. 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.”

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 first reinterpreted Sony in a way that significantly limited its scope. 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. 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 noninfringing. 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.”

The result is that the Sony defense is now an uncertain standard of unknown value. The original decision contemplated a bright-line rule that defeated all secondary liability claims. In some circuits, however,

---

161 Sony, 464 U.S. at 436-42.
162 Id. at 442.
163 Id. (“[W]e need not explore all the different potential uses of the machine[.]”)
164 Grokster, 545 U.S. at 957-58.
165 Lemley & Reese, supra note 17, at 1356-57.
166 A&M Records v. Napster, 239 F.3d 1004, 1020 (9th Cir. 2001); Tim Wu, The Copyright Paradox, 2005 SUP. CT. REV. 229, 234 (2005) (“One reading of Sony takes the language “merely capable” to create a presumption[.]”).
167 Aimster, 334 F.3d at 649-52.
168 Grokster, 545 U.S. at 933-34.
169 Olari, supra note 158, at 961 (noting that “doctrinally, the contours of Sony’s safe harbor remain vague”).

---
Sony applies only to contributory liability, and not to vicarious and inducement liability claims.\footnote{Högberg, supra note 139, at 927-28 & n.102.} 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. \textit{Other Efforts to Increase Uncertainty}

1. The Rise of Inducement Liability

Inducement liability is the third and most recent category of secondary copyright liability. When the Supreme Court initially created it in 2005, courts were unsure whether inducement was an independent category or a subset of contributory liability.\footnote{See, e.g., Columbia Pictures Indus. v. Fung, CV 06-5578 SVW(JCX), 2009 WL 6355911 (C.D. Cal. Dec. 21, 2009) (referring to inducement as a subset of contributory liability).} Most courts today, however, recognize it as an independent category.\footnote{See, e.g., Arista Records LLC v. Usenet.com, 633 F. Supp. 2d 124, 150-151 (S.D.N.Y. 2009).} Because of its recent origins, inducement liability has introduced significant uncertainty to secondary liability claims in several different respects. Viewing these cases through the lens of uncertainty, 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.\footnote{William Henslee, \textit{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, \textit{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.”).} These companies had strong arguments that they had no knowledge or control over users’ activities because they merely distributed software that users could use as they see fit (much like a VCR). At the same time, however, peer-to-peer services facilitated massive infringement. The Court’s challenge was to craft a holding that reached peer-to-peer services, but whose logic would not extend to other general-use technologies that
facilitate infringement (such as computers or operating system software).\textsuperscript{174}

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.”\textsuperscript{175} 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.

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 platforms on paper, the practical reality is that it creates a new standard that potentially justifies intrusive discovery.\textsuperscript{176} 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.\textsuperscript{177} 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.

These potential effects raise the important question of whether the DMCA safe harbor applies to inducement claims.\textsuperscript{178} 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,

\begin{footnotes}
\footnotetext{174}{Högberg, supra note 139, at 948-49.}
\footnotetext{175}{Grokster, 545 U.S. at 936-37.}
\footnotetext{176}{Wu, supra note 166, at 247-48.}
\footnotetext{177}{Grokster, 545 U.S. at 938-40.}
\footnotetext{178}{See generally Reese, supra note 157.}
\end{footnotes}
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.¹⁷⁹ 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.¹⁸⁰ The Second Circuit in YouTube also seemed to adopt this position, stating that “a finding of safe harbor application necessarily protects a defendant from all affirmative claims for monetary relief.”¹⁸¹ 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.¹⁸² 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.¹⁸³ 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.¹⁸⁴ In recent litigation, copyright owners have tried to expand the set of activities that give rise to direct infringement. These

¹⁷⁹ Fung, 2009 WL 6355911 at *18 (“[I]nducement liability and the Digital Millennium Copyright Act safe harbors are inherently contradictory.”).
¹⁸¹ YouTube, 676 F.3d at 41.
¹⁸² Id. at 38.
¹⁸³ CoStar Group, Inc. v. LoopNet, 373 F.3d 544, 555 (4th Cir. 2004) (“[T]he DMCA is irrelevant to determining what constitutes a prima facie case of copyright infringement.”)
¹⁸⁴ MDY Indus. v. Blizzard Entm’t, 629 F.3d 928, 941 (9th Cir. 2010). (“[S]econdary copyright infringement . . . requires the existence of direct copyright infringement.”).
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.” As background, courts have consistently held that “merely linking” to third-party content cannot establish direct infringement. In Perfect 10 v. Amazon.com, the Ninth Circuit extended this rule to Google’s “inline links,” which displayed images hosted on third-party servers. 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.” 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. 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.

A federal district court, however, recently held that video embeds can give rise to direct infringement. This holding, which contradicts virtually every known precedent, is currently on appeal and has captured

---


187 Id.

188 Id. at 1159.


the attention of major industry representatives such as Google, Facebook, and the MPAA. For our purposes, the most interesting aspect of the appeal is the interpretative dispute it creates. Internet platforms argue that the bright-line “server test” rule should apply to video embeds.\(^{192}\) The MPAA, by contrast, wants to replace this rule with a broader standard that allows video embeds (and other links) to constitute direct infringement. It further argues that these issues must be “decided on its facts.”\(^ {193}\) Again, the result here is arguably less important than the doctrinal standard the court adopts.

3. Suing Investors

The claim against Veoh’s investors represents a different type of effort to increase legal uncertainty.\(^{194}\) Its target was not legal doctrine per se, but the unwritten norms that shield digital technologies from secondary copyright liability. Norms are important because the doctrinal definitions of contributory and vicarious liability are so broad that they potentially extend to any digital technology used to infringe.\(^ {195}\) For instance, the logic of a case like *Napster* potentially applies to companies like Microsoft and Intel. The fact that these latter companies are not sued has less to do with doctrine, and more to do with implicit assumptions that these parties do not proximately facilitate infringement.

The Veoh investor suits, I argue, can be understood as attempts to unsettle these pre-existing norms in ways that expand secondary liability. Investors may have been aware that the *company* could be sued for infringement. They likely did not expect, however, to be sued themselves. In short, they relied on an unspoken norm that secondary liability did not extend to them. By suing the investors, the plaintiffs undermined this norm, and introduced new uncertainty into the law. And because investors are not “service providers,” they could not invoke the DMCA safe harbor.\(^ {196}\) In this respect, the litigation threatened to raise costs on all Internet platforms by causing investors to avoid platforms or to demand additional compensation for the risk.

---

\(^{192}\) *Google Flava Works Brief*, supra note 190, at 3-4.

\(^{193}\) *Brief of Amicus Curiae Motion Picture Association of America at 7-13 & n.7, Flava Works v. Gunter, No. 11-3190 (7th Cir. Nov. 30, 2011)*.


\(^{195}\) *See supra* note 140.

\(^{196}\) *See supra* note 66.
Recognizing these policy concerns, both the district court and the Ninth Circuit in *UMG* dismissed the investor suits before full discovery. The Ninth Circuit criticized the plaintiffs’ “novel theory of secondary liability,” which suggests the court viewed the suit as violating an established norm. Interestingly, both courts dismissed the claims by adopting clear holdings that would allow 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. The Ninth Circuit cited this premise to dismiss all three claims. The district court further found that general actions of board members do not rise to the level of “material contribution” or “direct financial benefit.” 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 section examines the efforts to institutionalize uncertainty within public enforcement proceedings. These efforts include both enacting new legislation that expands government authority, and interpreting existing statutory text in novel and expansive ways. The section 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. All computers on the Internet are assigned an IP (Internet Protocol) 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. 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. 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. Registrars 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.

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.

---

204 Id. at 1016-18.
206 Id.
207 Mellyn, supra note 202, at 1245-46. This is of course a simplified version of the process, but the more technical aspects of the DNS process is not necessary for our purposes.
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 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. 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. The statute itself, however, does not expressly reference domain names. Instead, Section 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. The government’s theory is that domain names are “property” that “facilitates” criminal copyright infringement. Indeed, many of the seized domain names direct 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).

2. Uncertainty Through New Legislation

The PRO-IP Act illustrates how Congress can expand the government’s enforcement authority by enacting vague uncertain 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

---


210 18 U.S.C. §2323(a)(1)(A)-(B). For convenience, I will refer to these provisions generically as “Section 2323(a).”

authority to seize tangible physical items like servers “used to provide the [infringing or counterfeit] services.”212 Similarly, critics of PRO-IP expressed concern about overbroad seizures of servers, along with a damages provision that was ultimately removed.213 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.214 Interestingly, this 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. Specifically, 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].”215 The accompanying committee report noted that violators’ use of “commercially valuable digital communications or e-commerce services” would not constitute facilitation “absent extraordinary circumstances.”216 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.217 On September 26, 2008, Senator Leahy introduced an amended bill. This bill—which is the

216 Id. at 41.
217 S. 3325, 110th Cong. §2 (2008) (as reported by S. Comm. on the Judiciary).
modern PRO-IP Act—no longer included the “substantial connection” language.218

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.219

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.

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.220 Rojadirecta organizes the links to sports streams into categories such as “Today on Internet TV,” and “Download Last Full Matches.”221 Rojadirecta does not host these streams, but instead links to third party sites that do.222 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.223

In February 2011, pursuant to a warrant, ICE (the Immigration and Customs Enforcement agency) seized Rojadirecta’s domain names under 218 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.

219 See infra Part III.B.


221 Rojadirecta Affidavit, supra note 32, at 37-38.


223 Temple, supra note 220.
Section 2323(a). The warrant alleged that Rojadirecta committed and facilitated criminal copyright infringement. Rojadirecta has challenged the seizures in court, arguing that they violate both Section 2323(a) and the First Amendment. In its pleadings, the government has offered two theories to justify its seizures under Section 2323(a). The first is that Rojadirecta is directly committing criminal infringement. The second is that Rojadirecta is facilitating criminal infringement. Under the latter approach, the government has argued that Rojadirecta’s criminal liability is irrelevant to the question of whether Rojadirecta facilitated infringement.

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.

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

---

224 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.

225 Rojadirecta Affidavit, supra note 32, at 45.

226 There are currently 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 v. United States, No. 11-3983 (S.D.N.Y. filed Jun. 13, 2011). This proceeding has been appealed to the Second Circuit. Puerto 80 Projects v. United States, No. 11-3390 (2d Cir. Aug. 19, 2011). The second involves the government’s motion for permanent forfeiture of the domain name. United States v. Rojadirecta.org, No. 11-4139 (S.D.N.Y. filed June 17, 2011). Because both proceedings raise similar legal issues, I combine them in the analysis below.


228 Government’s . . . Opposition to the Motion to [Dismiss] at 1, 9, United States v. Rojadirecta.org, No. 11-4139 (S.D.N.Y. Apr. 16, 2012) (“Puerto 80’s assertion that it is not itself directly liable . . . is wholly beside the point and utterly irrelevant[.]” (Gov. 2012 Opposition).
infringement. The government, however, has raised two arguments that potentially undermine this precedent. The first is that mere linking can constitute “aiding and abetting” criminal infringement. 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.

The potential benefits of these arguments become clear when viewed as an attempt to increase the uncertainty 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. Accordingly, it would 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. Although the government’s argument was seemingly narrow, the standard it advocated was quite broad. Specifically, the government’s preferred standard 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 loses this particular case, the standard—if accepted—would increase leverage against future defendants.

---

229 See supra note 183.
230 Gov. Opposition to Initial Petition, supra note 227, at 17, 21 (Rojadirecta has “aided and abetted the infringement by others[.]”).
231 Government’s . . . Opposition to the Motion to [Dismiss] at 12-13 n.7, United States v. Rojadirecta.org, No. 11-4139 (S.D.N.Y. Aug. 26, 2011) (Government 2011 Opposition);
In addition to linking, the government has other potential arguments that Rojadirecta’s actions constitute direct infringement. These arguments rely on an even more expansive reading of the criminal statutes. In some pleadings, for instance, the government argues that Rojadirecta “has engaged in contributory infringement.” Secondary liability, however, is not defined by statute, but is instead a judicial common law doctrine applicable to civil copyright cases. Because it is not statutorily defined, it cannot be a crime, and therefore cannot provide the basis for a Section 2323 seizure that requires underlying criminal activity. (In this respect, alleging accomplice liability provides a backdoor way of criminalizing civil secondary liability).

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 expanded and became more uncertain, they would necessarily enlarge the scope of criminal statutes as well.

One final dispute in the Rojadirecta proceeding is 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). In its pleadings, however, the government has instead urged a more objective standard that includes a “reckless disregard” of infringing activity. I do not provide a comprehensive analysis of willfulness here. For purposes here, the point is that the government prefers a broader standard that would potentially cover a wider range of activity.

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 Section 2323(a). Under this theory,
the government may seize domain names that facilitate infringement even if the website 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 Section 2323(a) avoids many of the expansions of the criminal statutes themselves discussed above. It does, however, dramatically expand the concept of “facilitation” under Section 2323(a). As Rojadirecta argued, the government’s theory attempts to “disaggregate seizure from any allegation of wrongdoing.”238 If wrongdoing is no longer required, it is—as Rojadirecta argues—difficult to find coherent limits to the government’s seizure authority.239 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 Section 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),240 while the Senate’s was the Protect IP Act of 2011 (PIPA).241 Congress ultimately dropped both bills in the face of intense controversy, but the bills will likely be revisited in future congressional sessions.242 The bills’ purpose was to target infringement

---

239 Id.
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.\textsuperscript{243} Specifically, both bills created obligations for—and enforcement remedies against—Internet Service Providers (ISPs), search engines, payment processors, and online advertisers.\textsuperscript{244}

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.\textsuperscript{245} 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.\textsuperscript{246} In this respect, the bills extend Section 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.\textsuperscript{247}

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.\textsuperscript{248} This language is virtually identical to the statutory text in Section 2323(a).\textsuperscript{249} By copying this language, SOPA potentially imports the same expansive

\textsuperscript{244} *SOPA*, §102(c)(2), 103(b); *PIPA* §3(d)(2), 4(d)(2).
\textsuperscript{245} *SOPA*, §102; *PIPA* §3.
\textsuperscript{246} *SOPA*, §102(b); *PIPA* §3(a).
\textsuperscript{247} *SOPA*, §102(c)(4); *PIPA* §3(e).
\textsuperscript{248} *SOPA* §102(a).
\textsuperscript{249} Compare 18 U.S.C. § 2323(a)(1)(A)-(B) with *SOPA* §102(a).
interpretations of “facilitation” that the government has used in the domain seizure cases.  

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.  
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.  

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.”  

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 “no duty to monitor.”  
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.  

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. 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 an unreasonable economic

---

250 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 Section 2323(a). Amendment in the Nature of a Substitute to H.R. 3261, at §102(a) (SOPA Manager’s Amendment).  

SOPA §102(c)(2); PIPA §3(d)(2).  

SOPA §102(c)(2)(A).  

SOPA Manager’s Amendment, supra note 250.  

SOPA §102(c)(2)(C)-(D).  


SOPA §102(c)(5); PIPA §3(d)(5).
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. 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. 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. 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. My focus, however, is on

---

257 SOPA, §102(c)(4); PIPA §3(e).


259 Corwin, supra note 7 (arguing that Megaupload indictment is more influential than SOPA and PIPA).

260 See supra notes 56-57.

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).

To review, Megaupload is a cyberlocker that stores files uploaded by its users, who could then share the files with the public. The government alleges that Megaupload is not a passive storage company, but instead actively encourages and facilitates massive copyright infringement. 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. 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. 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. Traditionally, however, these actions are governed by civil secondary liability doctrines. And because those doctrines are common law creations, they cannot establish criminal liability.

---

262 Sisario, supra note 5.
263 Megaupload Indictment, supra note 21, at ¶2.
264 Id. at 5.
266 Jennifer Granick, Megaupload: A Lot Less Guilty Than You Think, CIS BLOG, Jan. 26, 2012, available at 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.”).
267 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 7.
268 See supra note 234.
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 files. Indeed, courts have recently held that the latter practice—removing only the link—could not justify civil infringement.

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

The government’s prosecution of the owner of TVShack arguably expands criminal liability even further. 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. 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 has requested that O’Dwyer be extradited to the United States for prosecution.

The TVShack prosecution expands criminal liability by alleging that linking to third-party content can trigger prosecution. Although TVShack admittedly linked to infringing content, no one alleges that the site itself stored that content. The government’s theory implies that linking can justify criminal prosecution. As noted earlier, however, courts

269 Megaupload Indictment, supra note 21, at ¶¶4-23. For instance, James Grimmelmann observes that “much of what the indictment details are legitimate business strategies many websites use to increase their traffic and revenues.” Corwin, supra note 7.
270 MP3Tunes, 821 F. Supp. 2d at 639.
271 Megaupload Indictment, supra note 21, at ¶10.
272 Falzone & Granick, supra note 265 (“The indictment identifies a number of steps Megaupload took that appear designed to reduce rather than induce piracy.”).
274 Id. (“Mr. O’Dwyer's backers say his site was effectively a search engine.”).
276 Id. (“O’Dwyer's site was a ‘linking site’ that did not host infringing content itself.”).
have consistently held that mere linking cannot provide a basis for civil liability. In this respect, the TVShack prosecution extends enforcement authority a step beyond the domain name seizures, in which linking merely provided a “reasonable basis” for Section 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. 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. 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.”

IV. NORMATIVE ANALYSIS OF EXPANDED UNCERTAINTY

The previous sections explore how increased uncertainty effectively extends the scope of secondary copyright liability in both the civil and criminal contexts. It is not obvious, however, that this

---

277 See supra note 183.
279 See supra notes 56-57.
280 Falzone & Granick, supra note 265.
281 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 the platforms’ users. See supra note 266.
extension is normatively harmful. In many contexts, broad secondary liability is sound policy. This section, 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.

A. Policy Tradeoffs of Secondary Liability

Secondary liability—like copyright law more generally—involves policy tradeoffs. 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. 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. 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.


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.”).


In addition to increasing efficiency, secondary liability also promotes fairness.\footnote{Grossman, supra note 138, at 365-66 (“Simple fairness is arguably the overarching purpose of the rules”).} 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 greater financial resources than individual infringers.\footnote{See, e.g., Lynda J. Oswald, International Issues in Secondary Liability for Intellectual Property Rights Infringement, 45 AM. BUS. L.J. 247, 250 (2008).} 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.\footnote{Lichtman & Landes, supra note 282, at 397.} 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.\footnote{Netanel, supra note 283, at 16-17.} 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.\footnote{Lichtman & Landes, supra note 282, at 398.} 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. Further, the marginal cost of removing 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. 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. 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. 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 CATO research fellow Julian Sanchez has observed, the fact that these platforms are user-driven makes

---

293 For a comprehensive summary, see generally Barbara van Schewick, *INTERNET ARCHITECTURE AND INNOVATION* (2010).
294 *Id.* at 204-13 (discussing examples of relatively low cost innovation).
innovation occur more rapidly and in more unexpected ways.\textsuperscript{295} 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 you see what people do with it. . . . And 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.\textsuperscript{296}

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\textsuperscript{297} Although there is theoretical tension between copyright law and the First Amendment, courts have uniformly recognized that infringement is not protected speech.\textsuperscript{298} 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


\textsuperscript{296} Id.

\textsuperscript{297} Helman & Parchomovsky, supra note 36, at 1208-09.

referred to these threats as “censorship by proxy” in that it allows private parties to limit expression in ways government cannot.\textsuperscript{299}

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.\textsuperscript{300} For one, Internet platforms host an enormous and ever-changing amount of files.\textsuperscript{301} Further, it is often impossible for platforms to distinguish between infringing and non-infringing uses.\textsuperscript{302} 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 incentives to remove any material that copyright owners have identified—or may identify—as infringing. Indeed, one critique of the DMCA is that platforms owners already comply uncritically with content owners’ takedown requests.\textsuperscript{303} If the safe harbor becomes more uncertain, rational platforms will be even more aggressive in removing potentially infringing content.

Of course, copyright owners can object that the sheer volume of files makes it prohibitively costly for them to monitor platforms as well.\textsuperscript{304} 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

\textsuperscript{299} Kreimer, supra note 292, at 16-17; Seltzer, supra note 291, at 177-79; Wu, supra note 292, at 295-98.

\textsuperscript{300} UMG, 667 F.3d at 1037 (“Copyright holders know precisely what materials they own, and are thus better able to efficiently identify infringing copies than service providers like Veoh.”).

\textsuperscript{301} Lemley, supra note 135, at 101-02 (“Google has no realistic way of knowing which of the over 10 billion Web pages it searches might have information on it that violates the rights of someone else.”).

\textsuperscript{302} Helman & Parchomovsky, supra note 36, at 1211.

\textsuperscript{303} Alfred C. Yen, Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment, 88 Geo. L.J. 1833, 1888 (2000) (DMCA “encourage[s] ISPs to indiscriminately remove material from the Internet”).

\textsuperscript{304} Opening Brief of Plaintiffs-Appellants, at 31, Viacom Int’l v. YouTube, No. 10-3270 (2d Cir. Dec. 3, 2010) (“The consequences of the lower court’s view would be to have every copyright owner search every site on the Internet[.]”).
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 section, I propose measures to protect Internet platforms from uncertain secondary liability. Although I would welcome new clarifying 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 reduce legal uncertainty for Internet platforms facing 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 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.

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.

A. Increasing Certainty in Private Enforcement Actions

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.\(^{305}\) 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 Section 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.\(^{306}\) 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

---

305 Lee, supra note 67, at 262 (“[T]he DMCA safe harbors should be interpreted to promote clarity for private planning.”).

306 See supra note 77-78 and accompanying text.
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.\(^\text{307}\) In sum, courts wishing to protect platforms must interpret the DMCA as bright-line rules across the board.

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,\(^\text{308}\) while others—such as the “benefit and control” provisions—are worded as equitable standards.\(^\text{309}\) 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.\(^\text{310}\) 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,\(^\text{311}\) or to unreasonably alter their networks to accommodate copyright owners’ infringement protections.\(^\text{312}\)

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

---

\(^\text{307}\) As noted earlier, the Second Circuit creates significant uncertainty regarding the “willful blindness” and “benefit and control” provisions of the DMCA. *YouTube*, 676 F.3d at 34-35, 38.

\(^\text{308}\) 17 U.S.C. §512(c)(3) (notification procedures and requirements).


\(^\text{310}\) Helman & Parchomovsky, *supra* note 36, at 1207 (“[Safe harbors, by their very nature, are supposed to provide actors with certainty.”); Lee, *supra* note 67, at 262 (“An unclear ‘safe harbor’ is self-defeating and of no practical use[.]”).

\(^\text{311}\) 17 U.S.C. §512(m)(1).

\(^\text{312}\) 17 U.S.C. §512(i)(2)(C).
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.”

Examining some of the DMCA’s specific provisions illustrates how this general interpretative approach would apply in practice. The first provision is the “red flag knowledge” requirement. 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*. 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. 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—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. Textually, the provision is admittedly identical to common law vicarious liability standards. There are, however, several reasons to interpret it differently.

---

313 For examples in the Senate report, see S. Rep. 105-190, at 2 (“Title II will provide certainty”), 19 (Committee is sympathetic to the desire of such service providers to see the law clarified in this area”), 20 (safe harbor “provides greater certainty to service providers”); 40 (safe harbor “provides greater certainty to service providers”) (1998). For examples in the House report, see H.R. Rep. 105-551 Part 1, at 11 (DMCA “narrow[s] and clarify[i][es] the law” regarding secondary liability) (1998).

314 Id. at 11.


316 *UMG*, 667 F.3d at 1036-38; *YouTube*, 718 F. Supp. 2d at 525.

317 *MP3Tunes*, 821 F. Supp. 2d at 643.

318 *YouTube*, 676 F.3d at 34-35.

319 See supra note 148.
For one, interpreting the DMCA as co-extensive with the ever-expanding vicarious liability standard would effectively nullify the safe harbor.\(^{320}\) Such a reading is arguably inconsistent with the statute’s legislative history. Originally, the initial versions of Section 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.”\(^{321}\) The 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.\(^{322}\)

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.\(^{323}\)

An alternative approach would be to return to the roots of vicarious liability and interpret the provision as imposing an agency requirement.\(^{324}\) 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.\(^ {325}\) Under this approach, the ability to remove the

\(^{320}\) Lee, supra note 67, at 236-37 (noting “loophole” that potentially exists under this reading).


\(^{322}\) Id. at 11 (1998) (“[T]he current criteria for finding contributory infringement or vicarious liability are made clearer and somewhat more difficult to satisfy.”).

\(^{323}\) See supra note 153 and accompanying text.

\(^{324}\) Grossman, supra note 138, at 407-08; Högberg, supra note 139, at 935-36.

\(^{325}\) MP3Tunes, 821 F. Supp. 2d at 645; Io, 586 F. Supp. 2d at 1151 (“the pertinent inquiry is not whether Veoh has the right and ability to control it system, but rather, whether it has the right and ability to control the infringing activity”) (emphasis in original).
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. 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 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.

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. 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. My recommendation, accordingly, is that courts restore Sony’s original bright-line rule. 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.

326 See supra note 179.
327 See supra note 180-181 and accompanying text.
328 Napster, 239 F.3d at 1025; Fung, 2009 WL 6355911, at *15-18.
329 See supra Part II.B.
My proposal is that the Sony defense should be simple. If a device 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 device 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—although the Court sometimes confusingly referred to both as “vicarious liability.” 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 technologies 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 technologies 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. 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. 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...
defense would be available for other types of general-purpose technologies. 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 require a heightened pleading standard 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*, and *Grokster*, significant public evidence existed of their specific intent to promote infringement. This requirement would ensure that plaintiffs 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.” 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.

B. *Increasing Certainty in Public Enforcement Actions*

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 Section 2323(a), which would effectively prohibit domain name

---

333 *See, e.g., Grokster*, 545 U.S. at 937-38.
seizures under this statute. 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. 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 Section 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 Section 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.

A final possibility would not necessarily prevent seizures, but would instead allow sites to reclaim domain names quickly. Section 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.” 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. Courts, however, could interpret Section 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 Section 983(f) would not technically prevent seizures,

336 17 U.S.C. 509 (2006) repealed by PRO-IP Act, supra note 209; Eric Goldman, 16 No. 8 CYBERSPACE LAW, Sept. 2011, at 18 (“The applicable statute was designed to govern physical chattel, not virtual printing presses.”).
337 Puerto 80 Motion to Dismiss, supra note 234, at 11-12.
they could discourage them if site operators could immediately and reliably obtain their release.

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. 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. News reports have confirmed that the music and film industry played important roles in the Megaupload prosecution and the Dajaz1 domain name seizure. 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

340 See supra note 271-272 and accompanying text.
341 Goldman, supra note 265 (“[T]he government’s prosecution of Megaupload demonstrates the implications of the government acting as a proxy for private commercial interests”).
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 measure to combat foreign infringing sites called the OPEN Act. 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. 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. Indeed, this precise issue is being litigated in the Rojadirecta case before the Second Circuit. Because of space constraints, the First Amendment analysis is beyond the scope of this article, though I plan to explore it at length in a future project.

**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 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.”


344 Id.

345 See supra note 226.

In this respect, clarifying the law to protect Internet platforms will likely benefit all parties over time.