

10-1-2013

# Criminal Copyright Enforcement against Filesharing Services

Benton Martin

Jeremiah Newhall

Follow this and additional works at: <http://scholarship.law.unc.edu/ncjolt>Part of the [Law Commons](#)

---

## Recommended Citation

Benton Martin & Jeremiah Newhall, *Criminal Copyright Enforcement against Filesharing Services*, 15 N.C. J.L. & TECH. 101 (2013).  
Available at: <http://scholarship.law.unc.edu/ncjolt/vol15/iss1/5>

This Article is brought to you for free and open access by Carolina Law Scholarship Repository. It has been accepted for inclusion in North Carolina Journal of Law & Technology by an authorized administrator of Carolina Law Scholarship Repository. For more information, please contact [law\\_repository@unc.edu](mailto:law_repository@unc.edu).

**CRIMINAL COPYRIGHT ENFORCEMENT AGAINST FILESHARING  
SERVICES**

*Benton Martin and Jeremiah Newhall\**

*The high-profile prosecution of the popular online storage website Megaupload for criminal copyright infringement is the latest in a series of recent criminal prosecutions of online filesharing services. This Article addresses what pushes a legitimate online file-storing business over the edge to criminal enterprise, and how criminal copyright enforcement differs from civil enforcement. The Article first explains the history of criminal copyright enforcement in the United States. It then addresses why “secondary” theories of infringement apply in the criminal, as well as civil, context and why the DMCA “safe harbor” defense is a red herring in criminal copyright actions. It concludes by suggesting guidelines for prosecutorial discretion in enforcing criminal copyright law against filesharing services, proposing that prosecutions be limited to theories of liability already established in civil case law, and that prosecutors target only prominent filesharing-service operators that openly defy civil enforcement actions.*

---

\* Benton Martin is a law clerk to the Honorable Geraldine Soat Brown, Presiding Magistrate Judge for the Northern District of Illinois. Jeremiah Newhall is a litigator at the Vermont law firm of Ellis, Boxer & Blake PLLC, where his practice includes federal criminal defense. Previously, the authors clerked together in the staff attorney’s office of the Seventh Circuit. The views in this Article are those of the authors and in no way reflect the views of the judiciary. The authors wish to thank Julia Rickert, Andrew Moshirnia, Andrew Sellars, and most especially Meghan Martin and Karina Newhall.

## I. INTRODUCTION

In January 2012, an elite squad of New Zealand anti-terrorism officers, under the direction of the United States Department of Justice, stormed Kim Dotcom's lavish \$24-million mansion.<sup>1</sup> Equipped with body armor, tactical firearms, dog units, and a helicopter, the squad uncovered Dotcom hiding in a specially designed saferoom.<sup>2</sup> As he was whisked to a police van, Dotcom asked the charges against him. The answer was two words: "Copyright infringement."<sup>3</sup>

The indictment of Dotcom and his infamous filesharing service, Megaupload, marked the start of a new battle in what reporters have christened the "copyright wars."<sup>4</sup> Yet it is not the federal government's only recent foray into the fight against online filesharing services, which have been under a decade-long siege of civil litigation by media companies and the government because of these services' reputations as hotbeds for copyright infringement.<sup>5</sup> In 2010, for example, the Department of Homeland Security mounted "Operation in Our Sites" to seize the domain names of websites providing access to infringing content,<sup>6</sup> and the operation

---

<sup>1</sup> Charles Graeber, *10 Days Inside the Mansion—and Mind—of Kim Dotcom, the Most Wanted Man on the Internet*, WIRED (Oct. 18, 2012, 6:30 AM), <http://www.wired.com/threatlevel/2012/10/ff-kim-dotcom/>.

<sup>2</sup> *Id.*

<sup>3</sup> *Id.*

<sup>4</sup> Dan Mitchell, *Pirates Take Sweden*, N.Y. TIMES (Aug. 19, 2006), [http://www.nytimes.com/2006/08/19/business/19online.html?partner=rssnyt&emc=rss&\\_r=0](http://www.nytimes.com/2006/08/19/business/19online.html?partner=rssnyt&emc=rss&_r=0). Jack Valenti, president of the Motion Picture Association of America, has gone one step further, comparing efforts to force Internet service providers to remove infringing material to fighting a "terrorist war." Amy Harmon, *Black Hawk Download; Moving Beyond Music, Pirates Use New Tools to Turn the Net Into an Illicit Video Club*, N.Y. TIMES (Jan. 17, 2002), <http://www.nytimes.com/2002/01/17/technology/black-hawk-download-moving-beyond-music-pirates-use-new-tools-turn-net-into.html?pagewanted=all&src=pm>.

<sup>5</sup> NATE ANDERSON, *THE INTERNET POLICE: HOW CRIME WENT ONLINE, AND THE COPS FOLLOWED 199–202* (Nate Anderson ed., 2013) (documenting the history of this litigation).

<sup>6</sup> U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, 2010 U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR ANNUAL REPORT ON INTELLECTUAL PROPERTY ENFORCEMENT 4 (Feb. 2011), *available at*

has since resulted in the seizure of more than 400 domain names.<sup>7</sup> The issue more recently caught the attention of Congress, where bills were introduced in both the House and Senate to target foreign websites that link to or host infringing content.<sup>8</sup>

But these efforts have not always been effective. For many of the domain names seized by the Department of Homeland Security, the same infringing content quickly reappeared on sites with only slightly modified web addresses, and a few sites even grew in popularity.<sup>9</sup> And the backlash against the two new bills was fierce: a swarm of popular websites, including the online encyclopedia Wikipedia, staged a “blackout” in protest, citing fears that they would face sanctions merely for linking to controversial sites, even in informational articles.<sup>10</sup> Because of this opposition,

---

[http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec\\_annual\\_report\\_feb2011.pdf](http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_report_feb2011.pdf).

<sup>7</sup> U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, 2012 U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR JOINT STRATEGIC PLAN 1 (June 2012), *available at* [http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec\\_two-year\\_anniversary\\_report.pdf](http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_two-year_anniversary_report.pdf).

<sup>8</sup> See Mike Belleville, *IP Wars: SOPA, PIPA, and the Fight Over Online Piracy*, 26 TEMP. INT’L & COMP. L.J. 303, 303–04 (2012).

<sup>9</sup> Andy Sellars, *The In Rem Forfeiture of Copyright-Infringing Domain Names* 32 (Finnegan, Henderson, Farabow, Garrett & Dunner, LLP., Working Paper), *available at* [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1835604](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1835604). Onsmash.com moved to freeonsmash.com, for example, and increased from the 9520th most popular website in this country to the 7194th. *Id.*; see also Rob Fischer, *A Ninja in Our Sites*, THE AMERICAN PROSPECT (Dec. 15, 2011), <http://prospect.org/article/ninja-our-sites> (“Not surprisingly, the Spanish-based Rojadirecta enjoyed a sizable bump in traffic immediately following the seizure of its U.S.-based site.”); ANDERSON, *supra* note 5, at 217 (“Numerous site operators simply purchased new names not registered in the United States (www.ihatecopyright.eu, for instance) and continued with business as usual.”).

<sup>10</sup> Ned Potter, *Wikipedia Blackout: Websites Wikipedia, Reddit, Others Go Dark Wednesday to Protest SOPA, PIPA*, ABC NEWS (Jan. 17, 2012), <http://abcnews.go.com/Technology/wikipedia-blackout-websites-wikipedia-reddit-dark-wednesday-protest/story?id=15373251#.UNSZKax5Gq8>; Jenna Wortham, *With Twitter, Blackouts and Demonstrations, Web Flexes Its Muscle*, N.Y. TIMES (Jan. 18, 2012), [http://www.nytimes.com/2012/01/19/technology/protests-of-antipiracy-bills-unite-web.html?pagewanted=all&\\_r=0](http://www.nytimes.com/2012/01/19/technology/protests-of-antipiracy-bills-unite-web.html?pagewanted=all&_r=0).

the bills were quickly shelved.<sup>11</sup>

Meanwhile, other countries like Japan and Sweden have seen some success in directly prosecuting the operators of filesharing services. First, Japan convicted Isamu Kaneko, a computer-science researcher who developed Winny, an early peer-to-peer filesharing system.<sup>12</sup> Kaneko arguably fostered dubious uses of his service by collecting feedback and announcing updates through an anonymous Internet forum dedicated to filesharing.<sup>13</sup> Although Kaneko was convicted by a Japanese district court, the Osaka High Court reversed the conviction after concluding that Winny was “value neutral”—essentially, capable of non-infringing uses—and that Kaneko did not offer Winny primarily to promote infringement, even if he knew that it was probably being used for that purpose.<sup>14</sup> This decision touches on a key question in this Article: If a filesharing service is known to have rampant infringing uses, at what point do the service’s operators open themselves to criminal sanctions?

More successful was Sweden’s prosecution of the operators of The Pirate Bay, then one of the Internet’s largest peer-to-peer filesharing services.<sup>15</sup> The operators of The Pirate Bay mocked their contribution to infringing activity, often publishing and

---

<sup>11</sup> ANDERSON, *supra* note 5, at 221 (predicting that SOPA “will no doubt return” as the International Federation of the Phonographic Industry, a major international lobbying force for the recording industry, “still lists all of SOPA’s core provisions as key legislative priorities”).

<sup>12</sup> Salil K. Mehra, *Keep America Exceptional! Against Adopting Japanese and European-Style Criminalization of Contributory Copyright Infringement*, 13 VAND. J. ENT. & TECH. L. 811, 817 (2011).

<sup>13</sup> *Id.* at 816–17.

<sup>14</sup> *Id.* at 818–19 (citing Kyoto Chiho Saibansho [Kyoto Dist. Ct.] Dec. 13, 2006, Hei 16 (wa) no. 726, 1229 HANREI TIMES 105 (Japan), rev’d, Osaka Koto Saibansho [Osaka High Ct.] Oct. 8, 2009, Hei 19 (wa) no. 461 (Japan)).

<sup>15</sup> See Stephen Bright, *Current Development, The Current State of BitTorrent in International Law: Why Copyright Law is Ineffective and What Needs to Change*, 17 NEW ENG. J. INT’L & COMP. L. 265, 266 (2011); Jerker Edstrom & Henrik Nillson, *The Pirate Bay Verdict--Predictable, and Yet . . .*, 31 EUR. INTELL. PROP. REV., no. 9, at 483 (2009).

ridiculing complaints from copyright organizations.<sup>16</sup> Although Sweden once had a reputation for relaxed copyright laws, the country amended its Copyright Act in 2005 to make it a crime to transfer copyrighted content without permission.<sup>17</sup> When prosecutors then indicted four operators of The Pirate Bay in 2008 for “complicity” in violating the Act, the operators raised the same arguments as Kaneko—that their services had non-infringing uses, and that they were ignorant of any specific infringing activity.<sup>18</sup> The court nonetheless found the operators guilty, emphasizing that they had profited from infringing content by collecting advertising revenue and that knowledge of specific infringing content was unnecessary given that they had created conditions that fostered infringement and ignored notices of infringing content.<sup>19</sup> The defendants were each sentenced to one year in prison and ordered to pay restitution of \$4.3 million.<sup>20</sup>

The success of The Pirate Bay prosecution has been called a harbinger of actions like the one against Megaupload.<sup>21</sup> Yet criminal prosecution of filesharing services is a new development in the United States, and only time will tell whether this new approach proves effective, or under what circumstances it should be used. The future holds many questions. What pushes a legitimate online file-storing business into the territory of criminal enterprise? How might criminal copyright enforcement differ materially from civil enforcement? This Article seeks to answer

---

<sup>16</sup> Bright, *supra* note 15, at 277; Tara Touloumis, *Buccaneers and Bucks from the Internet: Pirate Bay and the Entertainment Industry*, 19 SETON HALL J. SPORTS & ENT. L. 253, 265 (2009).

<sup>17</sup> Bright, *supra* note 15, at 277; *see also* Bernard A. Mantel, *The Google Police: How the Indictment of The Pirate Bay Presents a New Solution to Internet Piracy*, 20 U. MIAMI BUS. L. REV. 77, 84 (2011).

<sup>18</sup> Mantel, *supra* note 17, at 85–87.

<sup>19</sup> *Id.* at 89 (citing Tingsrätt [TR] [Stockholm District Court] 2009-04-17 p. 1 B 13301-06 at 24 (Swed.), *as translated by* The International Federation of the Phonographic Industry, IFPI, [http://www.ifpi.org/content/section\\_about/index.html](http://www.ifpi.org/content/section_about/index.html)).

<sup>20</sup> *Id.* at 90–91.

<sup>21</sup> Bright, *supra* note 15, at 276–78; *see also* Mehra, *supra* note 12, at 822 (“The pressure to internationalize and harmonize the response to P2P also increases the possibility of American criminalization of contributory infringement.”).

these questions. It focuses on those online businesses enabling users to share infringing content with others online. These businesses will be referred to simply as “filesharing services,” with the intent that this definition covers diverse types of technology—including “cyberlockers” like Megaupload, which host files on servers controlled by the service, and “torrent” sites like The Pirate Bay, which provide links to connect users to infringing files stored by their peers.<sup>22</sup>

In the end, this Article concludes that criminal enforcement actions should be limited to the most notorious filesharing service operators that, in order to profiteer<sup>23</sup> from infringing content, foster infringement by egregiously defying the established boundaries of copyright law and civil means of copyright enforcement. Parts II and III of this Article describe the history of criminal copyright enforcement as well as significant developments in civil copyright law, clarifying the liability of filesharing services as secondary infringers. Part IV digs into the differences between the civil and criminal copyright landscape for filesharing services and the potential for “safe harbors” from criminal culpability for Internet service providers. Part V proposes guidelines for courts and prosecutors to consider when evaluating the propriety of a criminal enforcement action against filesharing services and discusses the procedural benefits to the government in criminal proceedings. Part VI concludes with a cautionary note about the powers available to prosecutors in this context.

---

<sup>22</sup> See generally Bill Wyman, *So Long, and Thanks for All the Pirated Movies*, SLATE (Jan. 20, 2012), [http://www.slate.com/articles/business/technology/2012/01/megaupload\\_shutdown\\_what\\_the\\_site\\_s\\_departure\\_means\\_for\\_other\\_traffic\\_hogging\\_cyberlockers.html](http://www.slate.com/articles/business/technology/2012/01/megaupload_shutdown_what_the_site_s_departure_means_for_other_traffic_hogging_cyberlockers.html) (discussing the function and business models of various cyberlocker sites). Cyberlockers like Megaupload in fact developed in part to give users more anonymity than torrent-type websites, which exposed users’ IP addresses to facilitate sharing. See ANDERSON, *supra* note 5, at 202–03. Cyberlockers, in contrast, offered direct downloads from a centralized server, guarding users’ IP addresses but increasing the difficulty in finding specific content. *Id.* at 203. In response, a number of “linking sites” developed to collect links to infringing content. *Id.*

<sup>23</sup> The profits at issue, however, must be in “real, non-Internet dollars.” *Brownmark Films, LLC v. Comedy Partners*, 682 F.3d 687, 694 (7th Cir. 2012). For more discussion of “Internet money,” see *id.* at 689.

## II. WAR BRIEFING: THE HISTORY OF CRIMINAL COPYRIGHT ENFORCEMENT

Criminal copyright enforcement against parties other than filesharing services is, of course, nothing new. The United States first criminalized copyright infringement in 1897 by making it a misdemeanor to conduct unauthorized performances of copyrighted plays and music—as long as this infringement was “willful and for profit.”<sup>24</sup> This law was intended to respond to complaints from copyright holders about the difficulty of enforcing their rights against troupes of traveling performers.<sup>25</sup> When traveling performers remained a problem a decade later, Congress expanded the law to punish all then-existing forms of copyright infringement and the people—primarily theater owners and agents—that aided or abetted infringers.<sup>26</sup>

Criminal copyright law remained unchanged until the 1970s, when concerns about piracy of sound and video recordings led to its rapid expansion.<sup>27</sup> The Sound Recording Act of 1971<sup>28</sup> first added protection for sound recordings.<sup>29</sup> Five years later, the 1976 Copyright Act<sup>30</sup> increased criminal fines for general infringement (up to \$10,000) and added even stiffer penalties for repeat infringers or infringers of sound recordings and motion pictures.<sup>31</sup> The 1976 Act also made repeat infringement a felony and changed the “for profit” requirement<sup>32</sup> to its current form—infringement

---

<sup>24</sup> Act of Jan. 6, 1897, ch. 4, 29 Stat. 481.

<sup>25</sup> I. Trotter Hardy, *Criminal Copyright Infringement*, 11 WM. & MARY BILL RTS. J. 305, 315 (2002) (citations omitted); see also Michael Coblenz, *Intellectual Property Crimes*, 9 ALB. L.J. SCI. & TECH. 235, 238–39 (1999).

<sup>26</sup> Copyright Act of 1909, ch. 320, 35 Stat. 1075; see Miriam Bitton, *Rethinking the Anti-Counterfeiting Trade Agreement's Criminal Copyright Enforcement Measures*, 102 J. CRIM. L. & CRIMINOLOGY 67, 85 (2012); see also Harv. L. Rev., Note, *Criminalization of Copyright Infringement in the Digital Era*, 112 HARV. L. REV. 1705, 1707 (1999).

<sup>27</sup> Bitton, *supra* note 26, at 85–86.

<sup>28</sup> Pub. L. No. 92-140, 85 Stat. 391 (1971).

<sup>29</sup> H.R. Rep. No. 93-1581, at 4 (1974), reprinted in 1974 U.S.C.C.A.N. 6849, 6852; see Harv. L. Rev., *supra* note 26, at 1708.

<sup>30</sup> Pub. L. No. 94-553, 90 Stat. 2541 (1976).

<sup>31</sup> See Harv. L. Rev., *supra* note 26, at 1709.

<sup>32</sup> Pub. L. No. 92-140, 85 Stat. 391 (1971).



“for purposes of commercial advantage or private financial gain”<sup>33</sup>—to clarify that infringers need only *intend* financial gain to be guilty.<sup>34</sup> Although the 1976 Act dropped all mention of “aiding and abetting” from the copyright statute, it appears that this change was intended merely to remove surplusage because this conduct remained a crime under 18 U.S.C. § 2.<sup>35</sup> More to the point, whether or not the intent was to remove surplusage, that was the effect: Aiding and abetting criminal copyright remains a crime under § 2(a).<sup>36</sup> This pattern of increasing penalties continued into the 1980s, as Congress responded to lobbying by the entertainment industry for even harsher criminal sanctions, in part by making first-time infringement, at least of significant quantities of audiovisual works, a felony.<sup>37</sup>

Unsurprisingly, popularization of personal computers and the Internet in the 1990s further spurred concerns about piracy, especially of software.<sup>38</sup> In response, Congress enacted the Copyright Felony Act of 1992,<sup>39</sup> expanding felony penalties to all types of copyright infringers and increasing the general maximum

---

<sup>33</sup> See 17 U.S.C. § 506(a)(1)(A) (2012).

<sup>34</sup> Irina D. Manta, *The Puzzle of Criminal Sanctions for Intellectual Property Infringement*, 24 HARV. J.L. & TECH. 469, 481 (2011); Harv. L. Rev., *supra* note 26, at 1708–09.

<sup>35</sup> 5 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT, § 15.01[A][2] (2013); Harv. L. Rev., *supra* note 26, at 1709 n.39.

<sup>36</sup> In fact, the statute covers not only aiding and abetting but willfully causing a crime to be committed by another:

(a) Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal. (b) Whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal.

18 U.S.C. § 2 (2012).

<sup>37</sup> Lydia Pallas Loren, *Digitization, Commodification, Criminalization: The Evolution of Criminal Copyright Infringement and the Importance of the Willfulness Requirement*, 77 WASH. U. L. Q. 835, 842–43 (1999).

<sup>38</sup> Harv. L. Rev., *supra* note 26, at 1711 (“Software manufacturers argued for stricter penalties for software copyright infringement, claiming that the piracy problems that had plagued the record and motion picture industry a decade ago were now attacking the software industry.”).

<sup>39</sup> Pub. L. No. 102-561, 106 Stat. 4233 (1992); *see also* 18 U.S.C. § 2319 (2012).

punishment for first-time offenders to five years' imprisonment, a \$250,000 fine, or both, as long as the infringer reproduced or distributed at least ten copies, worth more than \$2,500, within a six-month timeframe.<sup>40</sup> In 1996 Congress made counterfeiting copyrighted works a racketeering offense under the Racketeer Influenced and Corrupt Organizations Act.<sup>41</sup> Then in 1997 came the No Electronic Theft Act ("NET Act"),<sup>42</sup> a law that would foreshadow the Megaupload prosecution.

The impetus for the 1997 NET Act was a filesharing service that allowed free downloads,<sup>43</sup> conduct which is at the core of Megaupload's alleged infringement. Before the Act's enactment, the Department of Justice had attempted to convict student David LaMacchia for maintaining an online bulletin board full of infringing software files.<sup>44</sup> Because LaMacchia shared these files for free—and thus fell outside existing limits on criminal copyright liability—the government indicted him for wire fraud rather than copyright infringement. But a federal district court dismissed the case, relying on *Dowling v. United States*,<sup>45</sup> in which the Supreme Court overturned the conviction of a bootleg-record transporter as an impermissible subversion of carefully circumscribed copyright law.<sup>46</sup> Likewise, the *LaMacchia* court concluded, if not punishable under copyright law, nonprofit infringers should not be punished for wire fraud.<sup>47</sup> This controversial decision is widely reported to have motivated Congress's expansion of criminal copyright liability in the NET.<sup>48</sup> The Act sought to deter even not-for-profit infringement by expanding the definition of "financial gain" to cover "receipt, or expectation of receipt, of anything of value,

---

<sup>40</sup> Harv. L. Rev., *supra* note 26, at 1711–12.

<sup>41</sup> Anticounterfeiting Consumer Protection Act of 1996, Pub. L. No. 104-153, 110 Stat. 1386; *see* Manta, *supra* note 34, at 484.

<sup>42</sup> Pub. L. 105-147, 111 Stat. 2678 (1997).

<sup>43</sup> *See, e.g.*, Bitton, *supra* note 26, at 87; Manta, *supra* note 34, at 482.

<sup>44</sup> *United States v. LaMacchia*, 871 F. Supp. 535, 536–37 (D. Mass. 1994).

<sup>45</sup> *Dowling v. United States*, 473 U.S. 207 (1985).

<sup>46</sup> *LaMacchia*, 871 F. Supp. at 545.

<sup>47</sup> *Id.* at 543–44.

<sup>48</sup> *See, e.g.*, Bitton, *supra* note 26, at 87 ("Congress was thus spurred by the courts and the affected industries to broaden the scope of criminal liability to deter copyright offenders who had no financial motivation.").

including the receipt of other copyrighted works.”<sup>49</sup> The Act also added penalties for any willful infringer who reproduced or distributed \$1,000 worth of infringing copies, regardless of intended gain.<sup>50</sup>

Since that time, Congress has continued to ratchet up criminal copyright penalties. Discontent with the NET Act’s lack of deterrent effect, Congress enacted the Digital Theft Deterrence and Copyright Damages Improvement Act of 1999.<sup>51</sup> The Act’s approach was two-fold: It both increased the civil damages for copyright infringement and clarified that the United States Sentencing Commission would increase its recommended penalties for intellectual property crimes involving high-value or high-quantity infringement.<sup>52</sup> Then, in 2004 and 2005, Congress created the new copyright crimes of trafficking of counterfeit labels on protected works<sup>53</sup> and recording of motion pictures in theaters.<sup>54</sup> Finally, in 2008, Congress targeted counterfeiters again through the Prioritizing Resources and Organization for Intellectual Property Act (“PRO-IP Act”),<sup>55</sup> increasing criminal penalties for counterfeiting that may cause bodily injury (as with knock-off pharmaceuticals) and expanding the government’s power to seize counterfeit goods and the tools used to make them.<sup>56</sup>

---

<sup>49</sup> 17 U.S.C. § 101 (2012).

<sup>50</sup> *Id.* § 506 (2012); see also Harv. L. Rev., *supra* note 26, at 1715.

<sup>51</sup> Pub. L. No. 106-160, 113 Stat. 1774 (1999).

<sup>52</sup> Manta, *supra* note 34, at 483–84 (quoting H.R. REP. NO. 106-216, at 2 (1999)); see also Andrew W. Eichner, *File Sharing: A Tool for Innovation, or a Criminal Instrument*, 2011 B.C. INTELL. PROP. & TECH. F. 1 n.98 (2011) (citing H.R. 3456, 106th Cong. (1st Sess. 1999)).

<sup>53</sup> Anti-counterfeiting Amendments Act of 2004, Pub. L. No. 108-482, tit. I, 118 Stat. 3912, 3912–16.

<sup>54</sup> Artists’ Rights and Theft Prevention Act of 2005, Pub. L. No. 109-9, tit. I, 119 Stat. 218, 218–23. This Act was actually a sub-part of a larger piece of legislation titled the Family Entertainment and Copyright Act of 2005, Pub. L. No. 109-9, 119 Stat. 218–27.

<sup>55</sup> Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub. L. No. 110-403, § 1(a), 122 Stat. 4256.

<sup>56</sup> Beverley Earle, Gerald A. Madek, & Christina Madek, *Combating the New Drug Trade of Counterfeit Goods: A Proposal for New Legal Remedies*, 20 TRANSNAT’L L. & CONTEMP. PROBS. 677, 697–98 (2012). The PRO-IP Act also created a new executive position to coordinate federal copyright enforcement,

### III. RECENT COMBAT: ENFORCEMENT AGAINST FILESHARING SERVICES

While this discussion has focused thus far on criminal enforcement, much of the development of the application of copyright law to filesharing services has arisen in civil, rather than criminal, actions. Keystone developments include judicial recognition, through federal common law, of secondary liability for copyright infringement and relatively recent additions to digital piracy laws creating “safe harbors” for Internet service providers. Any discussion of criminal enforcement against filesharing services must therefore address parallel developments in civil litigation.

Perhaps the most significant statutory changes have been generated by the Digital Millennium Copyright Act (“DMCA”),<sup>57</sup> enacted a year after the NET Act in an attempt to balance media industry concerns over infringement with angst in the tech industry about hindering digital innovation.<sup>58</sup> Although the DMCA expanded the scope of criminal liability—making it a crime to circumvent, or traffic devices designed to circumvent, technological measures limiting access to copyrighted work<sup>59</sup>—the DMCA also created “safe harbors” for copyright infringement by various Internet businesses, including Internet service providers like Megaupload that host user-uploaded content.<sup>60</sup> The popular video-sharing site YouTube has used this relatively new doctrine in ongoing litigation brought against it by entertainment

---

the Intellectual Property Enforcement Coordinator, who is advised by representatives from the Register of Copyrights and the Criminal Division of the Department of Justice, among others. 15 U.S.C. § 8111(b)(3) (2012). The coordinator facilitates the creation and implementation of a Joint Strategic Plan. *Id.* § 8111(b)(1)(B).

<sup>57</sup> Pub. L. No. 105-304, 112 Stat. 2860 (1998).

<sup>58</sup> Harv. L. Rev., *supra* note 26, at 1717–18 (citing World Intellectual Property Organization Copyright Treaty, Dec. 20, 1996, 36 I.L.M. 65 (1997)); World Intellectual Property Organization Performances and Phonograms Treaty, Dec. 20, 1996, 36 I.L.M. 76 (1997); Statement by President William J. Clinton Upon Signing H.R. 2281, in 1998 U.S.C.C.A.N. 677, 677.

<sup>59</sup> 17 U.S.C. § 1201 (2012).

<sup>60</sup> *Id.* § 512(c); *see* *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 25 (2d Cir. 2012) (interpreting 17 U.S.C. § 512(c)).

companies,<sup>61</sup> successfully arguing that YouTube cannot be liable for infringing videos unless it first receives proper “takedown notices” about them.<sup>62</sup> This decision has given rise to speculation about the Megaupload defendants’ ability to avail themselves of this defense.<sup>63</sup> Notably, however, as discussed later, even if they otherwise met the provision’s requirements, the defense appears to be limited to civil actions alone.

YouTube is not the only company that has provoked litigation over its filesharing services. This litigation has led courts to address whether these services are liable as contributory and vicarious infringers, even though no statute explicitly endorses such secondary liability. The results are mixed. The Ninth Circuit, for example, concluded that the popular filesharing service Napster could be liable as a contributory infringer as long as it had actual knowledge of its users’ infringing activities.<sup>64</sup> But the Seventh Circuit disagreed, concluding that knowledge of infringement was not itself enough to hold liable a similar service called Aimster.<sup>65</sup> The Supreme Court, the Seventh Circuit noted, had decided two decades earlier that Sony was not liable when purchasers of its Betamax video recorder used it to create infringing copies of television programs, because the recorder was “widely used for

---

<sup>61</sup> See *Viacom Int’l*, 676 F.3d at 25–26.

<sup>62</sup> *Viacom Int’l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514 (S.D.N.Y. 2010). The Second Circuit affirmed the court’s core legal conclusion, although it took a different view of the evidence of YouTube’s knowledge of specific infringing videos, and reversed on that basis. See *Viacom Int’l*, 676 F.3d at 32–34.

<sup>63</sup> Graeber, *supra* note 1, at 193 (“But unlike the Viacom versus YouTube case, the charges against Megaupload are not civil but criminal; the key players aren’t being sued, they’re facing jail. Not for the first time, Kim finds himself embroiled in a criminal case based on uncertain tech precedent. Does safe harbor even apply in a criminal case? It’s not clear that a criminal statute against second-party copyright violation even exists. Welcome to the grayest gray zone on the Internet.”); Mantel, *supra* note 17, at 98 (“Today, the same charges as those against The Pirate Bay creators would not likely survive against Google in the United States. This is largely due to the fact that the DMCA exempts “service providers” from liability [under the safe-harbor provision].”) (internal citations omitted).

<sup>64</sup> *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1020 (9th Cir. 2001).

<sup>65</sup> *In re Aimster Copyright Litigation*, 334 F.3d 643, 649 (7th Cir. 2003).

legitimate, unobjectionable purposes.”<sup>66</sup> But even so, the Seventh Circuit concluded Aimster could not escape liability by willfully blinding itself to its users’ activities (through encryption software), especially because there was no evidence that the service was *ever* used for legitimate purposes.<sup>67</sup> The Seventh Circuit also expressed skepticism at the idea that Aimster might be vicariously liable—like a theater owner held liable for not policing infringing performers—but noted that sufficient evidence of contributory infringement, through willful blindness, made the question of vicarious liability merely academic.<sup>68</sup>

Eventually, the Supreme Court weighed in, concluding unanimously in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*<sup>69</sup> that Grokster and Streamcast—services that had sought to replace Napster in the wake of its litigation woes—could be liable as secondary infringers even without evidence that they knew about specific infringing videos.<sup>70</sup> The Court emphasized that these services had shown *intent* to promote infringement by, among other things, advertising themselves as alternatives to Napster and failing to develop filtering tools to curb infringement.<sup>71</sup> Despite these services’ potential many non-infringing uses, this evidence of intent to encourage infringement, the Court reasoned, distinguished these services from Sony’s Betamax, the last technology it had addressed regarding secondary infringement.<sup>72</sup>

---

<sup>66</sup> Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984).

<sup>67</sup> *In re Aimster*, 334 F.3d at 650–53.

<sup>68</sup> *Id.* at 654–55.

<sup>69</sup> 545 U.S. 913 (2005).

<sup>70</sup> *Id.* at 932–34.

<sup>71</sup> *Id.* at 938–39. The Court observed that “Grokster’s name is apparently derived from Napster.” *Id.* at 939. Although not noted by the Court, Grokster is an apparent portmanteau of “Grok” and “Napster”; the former is a neologism by Robert Heinlein meaning “[t]o understand intuitively or by empathy.” J.A. SIMPSON & E.S.C. WEINER, THE OXFORD ENGLISH DICTIONARY VOLUME VI, 864 (2d ed. 1989); see also ROBERT A. HEINLEIN, STRANGER IN A STRANGE LAND 213 (Ace mass-market ed. 1987) (“[If] you grok it, understand it so thoroughly that you merge with it and it merges with you.”). Grokster’s name conveyed to fans of Napster that Grokster understood and empathized with them. *Id.*

<sup>72</sup> *Grokster*, 545 U.S. at 933–35.

As explained later, this focus on intent causes the standard for secondary civil copyright liability to approach alignment with the willfulness standard for criminal copyright culpability.<sup>73</sup>

It was only a matter of time, then, before federal prosecutors—buoyed by *Grokster*'s endorsement of secondary liability and Sweden's successful conviction of The Pirate Bay—sought criminal penalties for filesharing services. The first of these efforts began in 2010, as the United States targeted NinjaVideo (a service as much about direct infringement as secondary), which was created to showcase collections of infringing content uploaded by its founder Hana Beshara.<sup>74</sup> NinjaVideo collected more than \$500,000 in advertising revenue and donations for providing links to user-uploaded content—some of it stored on Megaupload's servers.<sup>75</sup> As part of the NinjaVideo investigation, the Department of Justice obtained a search warrant for Megaupload-controlled servers in Virginia, gathering evidence leading to the indictment of Beshara, who pleaded guilty and was ordered to serve 22 months in prison and pay \$200,000 in restitution.<sup>76</sup>

The government also pursued the operators of two services—TVShack.net and channelsurfing.net—that provided links to (often

---

<sup>73</sup> This alignment is particularly acute if, as Professor Timothy Holbrook argues, *Grokster* is read to require intent to induce infringement rather than merely intent to induce the acts. See Timothy R. Holbrook, Symposium Review, *The Intent Element of Induced Infringement*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 399, 408 (2006).

<sup>74</sup> Fischer, *supra* note 9.

<sup>75</sup> Timothy B. Lee, *How the Criminalization of Copyright Threatens Innovation and the Rule of Law*, in COPYRIGHT UNBALANCED: FROM INCENTIVE TO EXCESS 63–64 (Jerry Brito ed., 2012); David Kravets, *Megaupload Assisted U.S. Prosecution of Smaller File-Sharing Service*, WIRED (Nov. 20, 2012, 2:54 PM), <http://www.wired.com/threatlevel/2012/11/megaupload-investigation-roots/>.

<sup>76</sup> Press Release, Dep't of Justice, *Leader of NinjaVideo.net Website Sentenced to 22 Months in Prison for Criminal Copyright Conspiracy* (Jan. 6, 2012), <http://www.justice.gov/usao/vae/news/2012/01/20120106ninjavideonr.html>. Query whether this prosecution primarily served to build a case against Megaupload is already under investigation by U.S. officials. Kravets, *supra* note 75.

infringing) streaming video of copyrighted television shows.<sup>77</sup> But as the Seventh Circuit noted recently, in rejecting a preliminary injunction against a “social bookmarking” site, myVidster, the liability of services allowing users to post infringing links to content hosted by third-parties is a particularly close question, turning on the extent of the service’s contribution to, and intent to encourage, infringement.<sup>78</sup> Thus, the case against the operator of channelsurfing.net stalled, and the initially approved extradition of TVShack.net’s British creator faltered on appeal, prompting the United States to offer deferred prosecution in exchange for him paying a small fine.<sup>79</sup> By that time, however, the government had mounted its case against Megaupload—a file-hosting rather than link-listing site—which, according to the indictment, was the “13th most frequently visited website on the entire Internet.”<sup>80</sup>

#### IV. NEW BATTLEFIELDS: CHALLENGES IN PROSECUTING FILESHARING SERVICES

This Article now turns to evaluating what this history means for online filesharing services going forward. Here, the indictment against Megaupload becomes a valuable guide, serving as a looking glass into the future of criminal copyright liability for this type of online business.<sup>81</sup> The indictment charges the defendants, as part of a “Mega Conspiracy,” with committing six different federal crimes.<sup>82</sup> Two of these crimes derive from allegations that

---

<sup>77</sup> Timothy B. Lee, *UK TV Shack admin won't face trial in US on copyright charges*, ARS TECHNICA (Nov. 28, 2012), <http://arstechnica.com/tech-policy/2012/11/uk-tv-shack-admin-wont-face-trial-in-us-on-copyright-charges/>. Channel Surfing’s operator was indicted in 2011, and the case is still ongoing. Fischer, *supra* note 9; United States v. McCarthy, 1:11-cr-00900-TPG, ECF Doc. 15 (S.D.N.Y. Oct. 21, 2011).

<sup>78</sup> See *Flava Works, Inc. v. Gunter*, 689 F.3d 754 (7th Cir. 2012).

<sup>79</sup> See Lee, *supra* note 75; ANDERSON, *supra* note 5, at 223.

<sup>80</sup> United States v. Dotcom, No. 1:12-CR-3, ECF Doc. 34, at 2 (E.D. Va. Feb. 16, 2012) [hereinafter Indictment], *available at* <http://www.washingtonpost.com/wp-srv/business/documents/megaupload-indictment.pdf>.

<sup>81</sup> *Id.*

<sup>82</sup> *Id.* The six crimes include conspiracy to commit racketeering (18 U.S.C. § 1962(d) (2012)), conspiracy to commit copyright infringement (*id.* § 371), conspiracy to commit money laundering (*id.* § 1956(h)), criminal copyright infringement by distributing a copyrighted work being prepared for commercial



the defendants aided and abetted infringers, along with directly infringing copyright themselves.<sup>83</sup> Others involve conspiracies flowing from this infringing activity.<sup>84</sup> Finally, the indictment charges wire fraud, a white-collar-crime standby, because the defendants allegedly conned copyright holders into believing their works were being removed after takedown complaints.<sup>85</sup>

But the true *sine qua non* of the Megaupload prosecution is criminal copyright infringement, just as the police told Kim Dotcom at his arrest.<sup>86</sup> That crime has three elements: (1) willful (2) infringement (3) for commercial advantage or financial gain.<sup>87</sup>

---

distribution on a computer network and aiding and abetting of criminal copyright infringement (*id.* §§ 2, 2319; 17 U.S.C. § 506 (2012)), criminal copyright infringement by electronic means and aiding and abetting of criminal copyright infringement (18 U.S.C. §§ 2, 2319; 17 U.S.C. § 506), and fraud by wire and aiding and abetting of fraud by wire (18 U.S.C. §§ 2, 1343).

<sup>83</sup> Indictment, *supra* note 80, at 71–76. These accusations actually constitute counts four to eight of the indictment; five to eight allege multiple violations of 18 U.S.C. §§ 2 and 2319, and 17 U.S.C. § 506. Indictment, *supra* note 80, at 71–76.

<sup>84</sup> Indictment, *supra* note 80, at 22–71.

<sup>85</sup> *Id.* at 77–80 (these accusations constitute counts nine to thirteen, which allege five separate violations of 18 U.S.C. §§ 2 and 134).

<sup>86</sup> See *supra* note 1.

<sup>87</sup> 17 U.S.C. § 506(a)(1) (2012). The relevant text of the statute:

(a) Criminal infringement.--

(1) In general.--Any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed--

(A) for purposes of commercial advantage or private financial gain;

(B) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than \$1,000; or

(C) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution.

*Id.* As noted *supra* Part I, copying or distribution of copyrighted works with a value of more than \$1,000 would also satisfy the third element, as would distribution of a yet-unreleased work being prepared for commercial distribution (i.e. an unreleased film). See *id.*; see also 5 NIMMER & NIMMER, *supra* note 35, at § 15.01.

This section will focus on the interplay of the first two elements; the former is unique to criminal prosecutions, and the latter imports to the criminal law most of the defenses to civil liability.<sup>88</sup> Applying these elements requires applying them *to* something, and so it is a worthy diversion to examine just what underlying infringement the indictment actually alleges.

First, there are charges of direct infringement. The indictment charges Megaupload employees with uploading copies of copyrighted works, such as the film “Taken.”<sup>89</sup> The application of the elements of infringement to that conduct, if proven, will be straightforward: The government alleges that Megaupload copied these works for financial gain, with full knowledge that they were under copyright.<sup>90</sup>

---

<sup>88</sup> See 5 NIMMER & NIMMER, *supra* note 35, at § 15.01(A).

<sup>89</sup> In “Taken,” Oscar<sup>TM</sup>-winner Liam Neeson portrays Bryan Mills, a retired CIA black-ops agent and the father of a kidnapped woman. On the phone with the kidnappers, Mills tries to dissuade them from taking his daughter:

I don’t know who you are. I don’t know what you want. If you are looking for ransom, I can tell you I don’t have money. But what I do have are a very particular set of skills; skills I have acquired over a very long career. Skills that make me a nightmare for people like you. If you let my daughter go now, that’ll be the end of it. I will not look for you, I will not pursue you. But if you don’t, I will look for you, I will find you, and I will kill you.

TAKEN (20th Century Fox 2009). Since the film’s premiere, the “Taken” speech has become a popular meme, with people paraphrasing it to dissuade lunch thieves (“I don’t know who you are. I don’t know what you want. If you are looking for cherry cola, I can tell you that I don’t have any because some unscrupulous beast drank mine.”), to break up with a passive-aggressive boyfriend, (“But what you do have are a very particular set of passive-aggressive skills; skills that make you a nightmare for girlfriends like me.”), or to ban armchair grammarians from their Facebook page (“If you let my grammatical error go now, that’ll be the end of it . . . But if you don’t, I will hide you, I will unsubscribe from you, and I will unfriend you.”). See *Using the “Taken” Speech In Every Aspect of Your Life*, HAPPYPLACE (Oct. 3, 2012), <http://www.happyplace.com/18230/how-to-behave-like-liam-neeson-in-taken-in-every-aspect-of-your-life>. In that spirit, this Article offers a caveat to copyright infringers. Prosecutors may not know who you are, and they may not have jurisdiction, but what they do have are a very particular set of powers; powers that include extradition. They will look for you, they will find you, and they will extradite you.

<sup>90</sup> See Indictment, *supra* note 80, at 49.

Like Grokster and Napster, the bulk of Megaupload's alleged infringement liability is secondary; that is, Megaupload is not charged with committing most of the alleged infringement itself,<sup>91</sup> but rather with aiding and abetting infringement by others.<sup>92</sup> Who, then, are the actual infringers? At first blush, Megaupload's viewers might appear to be the infringers because they stream unlicensed broadcasts of copyrighted content. But each of the thousands, possibly millions,<sup>93</sup> of unauthorized viewers of copyrighted works on Megaupload "is no more a copyright infringer than if he had snuck into a movie theater and watched a copyrighted movie without buying a ticket."<sup>94</sup> The only other candidates—the only other people involved—are the uploaders of the infringing material. Yet, uploading copyrighted material to a remote server, an activity widely promoted by technology and media companies heralding the future of cloud computing, is as much a fair use as is recording a program for later viewing.<sup>95</sup>

---

<sup>91</sup> *Id.* at 12 (alleging that a handful of Megaupload employees uploaded infringing copies of works).

<sup>92</sup> See *supra* notes 82–85 and accompanying text.

<sup>93</sup> The indictment summarizes the potential breadth of infringing activity on Megaupload:

Megaupload.com was at one point in its history estimated to be the 13<sup>th</sup> most frequently visited website on the entire Internet. The site claims to have had more than one billion visitors in its history, more than 180,000,000 registered users to date, an average of 50 million daily visits, and to account for approximately four percent of the total traffic on the Internet.

Indictment, *supra* note 80, at 2–3.

<sup>94</sup> *Flava Works, Inc. v. Gunter*, 689 F.3d 754, 758 (7th Cir. 2012). Query whether Judge Posner's metaphor of sneaking into a movie theater withstands closer inspection. The actual performance in this case, as well as in *Flava Works*, is started and stopped not by the uploader (or, in that case, the copyright holder) but by the person streaming the video. Why should the uploader be *directly* liable, as opposed to *secondarily* liable, for an infringing performance started and stopped by someone else? But whatever the answer, *someone* has violated the copyright holder's right of performance, and Megaupload stands accused of encouraging uploaders and viewers alike.

<sup>95</sup> See *Sony Corp. of Am., Inc. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984); see also *In re Aimster Copyright Litig.*, 334 F.3d 643, 647 (7th Cir. 2003).

Although copying a work onto a remote server alone would not be a crime, copying is not the only exclusive right of copyright holders; they also have the exclusive right of performance, which includes broadcasts of audiovisual works.<sup>96</sup> So, it is not the uploader's copying but their *sharing* of the stored file with others that violates the copyright act, and *that* is the primary infringement that Megaupload is alleged to have aided and abetted.<sup>97</sup>

A few commentators have argued that there should be *no* criminal liability for filesharing services for the copyright infringement of their users. Their argument treats the prosecution's theory—to the extent it seeks to hold the Mega-conspirators liable for conduct other than their own infringing uploads—as an overextension of the doctrine of secondary infringement endorsed by the Supreme Court in *Grokster*.<sup>98</sup> To some extent, this position reflects hostility to the strength of United States copyright protections generally, rather than a principled distinction between *Grokster* and the Megaupload prosecution. But there is some substance to the argument that judges are free to create various theories of liability in civil law, but not in criminal

---

<sup>96</sup> See 17 U.S.C. § 106(4) (2012); 2 NIMMER & NIMMER, *supra* note 35, at § 8.14; *Flava Works, Inc.*, 689 F.3d at 758 (“The right to control copying is not the only exclusive right of a copyright owner. That would make life too simple for us.”).

<sup>97</sup> Although the indictment charges Megaupload with secondary liability for “distribution,” a right codified in § 106(3), it is inapplicable to Megaupload unless the works were downloaded, as opposed to streamed. “Downloading” creates a permanent copy of the video file on the computer’s hard drive. “Streaming” is a process by which a computer makes a temporary “buffer” copy of a video file, which is destroyed as the video is played. See JOHN C. DVORAK, CHRIS PIRILLO & WENDY TAYLOR, *ONLINE! THE BOOK* 399 (2003). If the government intends to prove infringement by “distribution,” *then* the primary infringers would be the individuals who downloaded copies.

<sup>98</sup> Lee, *supra* note 75, at 67–70 (arguing that secondary liability should not be extended in the criminal context because the doctrine has been fleshed out by the courts not Congress); Jennifer Granick, *Megaupload: A Lot Less Guilty Than You Think*, THE CENTER FOR INTERNET AND SOCIETY BLOG (Jan. 26, 2012, 11:47 AM), <http://cyberlaw.stanford.edu/blog/2012/01/megaupload-lot-less-guilty-you-think> (“But the first question from a defense perspective has to be ‘Can the Grokster theory of CIVIL liability even be the basis for CRIMINAL copyright claims?’ This has never been decided by any Court.”).

law.<sup>99</sup> In fact, the rule of lenity reflects a judicial willingness to find *exceptions* to liability in criminal law.<sup>100</sup> So where can “vicarious,” “contributory,” or “inducement” liability be found in the statute?

All of these civil liability theories fall under the umbrella term of “secondary liability” and correlate with variants of “aiding and abetting” under 18 U.S.C. § 2.<sup>101</sup> As the Seventh Circuit noted in *Aimster*, *Sony* treats “vicarious and contributory infringement interchangeably.”<sup>102</sup> Although *Grokster* purports to give the two terms distinct definitions, postulating that a person “infringes contributorily by intentionally inducing or encouraging direct infringement and infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it.”<sup>103</sup> But the decision strips away this definitional clarity in a footnote, quoting *Sony*’s conclusion that “‘the lines between direct infringement, contributory infringement and vicarious liability are not clearly drawn.’”<sup>104</sup> On top of that, the Supreme Court

---

<sup>99</sup> See RICHARD A. POSNER, HOW JUDGES THINK 48 (2008) (positing that even most legalists are “willing to allow common law judges (and almost all American judges have a common law as well as a statutory and constitutional jurisdiction) to overrule and distinguish precedents and create new common law rules and standards”); see also ANTONIN SCALIA & BRYAN A. GARNER, READING LAW: THE INTERPRETATION OF LEGAL TEXTS 319 (2012) (distinguishing judge-made, policy-driven changes to the common law from changes of the same ilk to statutory law, and finding only the former permissible).

<sup>100</sup> See, e.g., *United States v. Costello*, 666 F.3d 1040, 1048 (7th Cir. 2012) (“We mustn’t forget the rule of lenity in the interpretation of criminal statutes, or the words of the great nineteenth-century English jurist of criminal law James Fitzjames Stephen: ‘Before an act can be treated as a crime, it ought . . . to be of such nature that it is worthwhile to prevent it at the risk of inflicting great damage, direct and indirect, upon those who commit it.’”) (citations omitted); see also SCALIA & GARNER, *supra* note 99, at 296–302 (advocating application of rule of lenity as a “canon of construction”).

<sup>101</sup> See 18 U.S.C. § 2 (2012). The statute actually covers much more than “aiding and abetting,” and this Article uses the phrase as shorthand for all of the conduct covered in § 2. See *id.*

<sup>102</sup> *In re Aimster Copyright Litig.*, 334 F.3d 643, 654 (7th Cir. 2003).

<sup>103</sup> *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 930 (2005) (internal citations omitted).

<sup>104</sup> *Id.* n.9.

concluded that it need not analyze the question of vicarious liability because it was resolving the case “based on an inducement theory.”<sup>105</sup> To avoid this confusion, this Article lumps together vicarious, contributory, or induced infringement as different permutations of a single claim of “secondary liability.”<sup>106</sup>

Because aiding and abetting is the criminal corollary to secondary liability,<sup>107</sup> this Article proposes that the two concepts should cover the same conduct. All of the variant theories of secondary liability boil down to intentionally encouraging others to infringe, or helping them to do so. In the criminal context, that same conduct is referred to as aiding and abetting. And unlike vicarious, contributory, or inducement liability, aiding and abetting is a creature of statute,<sup>108</sup> so no common law theories of liability are required.

But prosecuting Megaupload (or anyone else) for aiding and abetting copyright infringement requires defining precisely what activity the government must prove that a filesharing service aided. One approach would be to make the government prove that the underlying infringement was also criminal, meeting the same standard of willfulness. That would force the government to prove that at least one user willfully and for commercial advantage

---

<sup>105</sup> *Id.*

<sup>106</sup> See, e.g., Pamela Samuelson, *Is Copyright Reform Possible?*, 126 HARV. L. REV. 740, 775 (2013) (book review) (“Through a common law process, courts have developed three different theories of secondary liability: one for contributory infringement, one for vicarious liability, and one for inducing infringement.”); Jay Dratler, Jr., *Common-Sense (Federal) Common Law Adrift in a Statutory Sea, or Why Grokster was a Unanimous Decision*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 413, 437 (2006) (“If it were up to me, I would junk all the terms ‘inducement,’ ‘vicarious liability’ and ‘contributory infringement’ in referring to a legal cause of action and use a single, consistent term—‘secondary liability’—for all claims of this kind.”).

<sup>107</sup> *In re Aimster*, 334 F.3d at 651 (“There are analogies in the law of aiding and abetting, the criminal counterpart to contributory infringement.”); *Perfect 10, Inc. v. Visa Int’l Serv. Ass’n*, 494 F.3d 788, 815 (9th Cir. 2007) (Kozinski, J., dissenting); Jacqueline C. Charlesworth, *The Moral of the Story: What Grokster Has to Teach About the DMCA*, 2011 STAN. TECH. L. REV. 6, 43–46 (2011); cf. *Flava Works, Inc. v. Gunter*, 689 F.3d 754, 755 (7th Cir. 2012) (describing a secondary infringer as “roughly an infringer’s accomplice”).

<sup>108</sup> 18 U.S.C. § 2 (2012).

infringed a copyright. The government would not have to *convict* anyone of that underlying infringement in order to convict operators of a filesharing service, but it would have to prove that the infringement happened. Think of prosecuting someone for aiding and abetting a bank robbery: Prosecutors must prove the robbery happened, even if they never prosecute the actual robber.<sup>109</sup> And a good defense attorney will argue that part of the crime of robbery is intent, just as part of the crime of copyright infringement is willfulness. So, does the government have to prove that unnamed users “willfully” infringed the uploaded works, in addition to proving that operators of a filesharing service willfully aided them?

Although some copyright scholars have latched onto this dubious theory,<sup>110</sup> the answer is clearly “No.” Criminal law is not an endless fractal of intent, delving down and down like Alice’s rabbit hole. Once again, it helps to think of aiding and abetting a crime in the “analog” world, such as robbery. Others have been quick to point out that driving a robber to a bank is not a crime if the driver has no knowledge of the robbery.<sup>111</sup> But the reverse also holds: If someone drives the Joker<sup>112</sup> to Gotham Bank knowing

---

<sup>109</sup> See, e.g., *United States v. Powell*, 806 F.2d 1421, 1424 (9th Cir. 1986) (“The government correctly points out that a defendant can be convicted of aiding and abetting even if a principal is never identified or convicted. Nonetheless, a defendant cannot be criminally convicted absent proof that a principal criminal offense was committed.”) (internal citations omitted).

<sup>110</sup> See, e.g., Rick Sanders, *Megaupload: Legal Obstacle Course for Prosecutors: Copyright*, AARON SANDERS PLLC (Feb. 27, 2012), <http://www.aaronsanderslaw.com/blog/megaupload-legal-obstacle-course-for-prosecutors-copyright>.

<sup>111</sup> See *id.* (“If your buddy just asked you for a ride to the bank . . . , you wouldn’t be aiding and abetting the bank robbery.”).

<sup>112</sup> Although in this hypothetical the Joker (clown-faced nemesis of comic-book hero Batman) is robbing a bank, he is also no stranger to copyright crime—although of an unusual kind. The Joker once dumped chemicals into Gotham Bay that mutated all of the fish; these mutant fish wore toothy grins with white faces—reminiscent of the Joker’s own face. Dubbing them “Joker Fish,” the Joker plotted to get rich by copyrighting them and earning a royalty from every fish stick. But when he broke into the office of the Commissioner of Copyright, the Commissioner refused to register his work, insisting: “Nobody can copyright fish—or even fish faces! They’re a natural resource!” The Joker

that he will commit a robbery, but the Joker is acquitted by reason of insanity, his inability to understand the consequences of his actions does not acquit the driver.<sup>113</sup> Returning to the digital world of online copyright infringement, if operators of a filesharing service willfully assist users in infringement, the users' subjective belief that their uploads are a fair use (if they indeed hold such a belief) would not protect the services' operators<sup>114</sup>—Nor should it. Otherwise, ignorance of the primary infringer would be a shield, and cunning criminals could use the naïve as unwitting tools of crime.

The challenges to extending “secondary liability” to criminal copyright law are overblown. Although Megaupload may have a stronger defense, as discussed herein, the allegations that Megaupload knowingly assisted widespread infringement for profit would, if proven, easily constitute criminal aiding and abetting of that infringement.

Allegations are not proof, however, and the government will have a high bar to clear. To win its case against Megaupload, the government must prove the same facts required for a civil lawsuit, but it must prove them beyond a reasonable doubt (as opposed to the civil standard of preponderance of the evidence), and it must prove that the infringement was willful and for commercial gain.<sup>115</sup> Because the government must prove the same facts (plus one more—willfulness), most of the same defenses available in a civil lawsuit are also available in a criminal prosecution, including fair

---

was unmoved: “But the fish share my unique face! If colonel what’s-his-name can have chickens, when they don’t even have mustaches--! And you deny this to me! You see why I am forced to crime!” See Steve Englehart & Marshall Rogers, *The Laughing Fish!*, BATMAN’S DETECTIVE COMICS 475, at 9–10 (DC Comics Feb. 1978).

<sup>113</sup> 18 U.S.C. § 2(b) (2012).

<sup>114</sup> Chris Dodd, head of the Motion Picture Association of America, has used a similar analogy in discussing search engines’ potential liability for copyright infringement: “How do you justify a search engine providing for someone to go and steal something? A guy that drives the getaway car didn’t rob the bank necessarily, but they got you to the bank and they got you out of it, so they are accessories in my view.” ANDERSON, *supra* note 5, at 219.

<sup>115</sup> Or, as noted, the value of the works infringed in a six-month period exceeded \$1,000. 17 U.S.C. § 512(a) (2012).



use, implied license, and abandonment of copyright. A handful of defenses available in civil actions are, however, inapplicable to criminal prosecution—most notably, the failure to register a work with the copyright office and the DMCA’s safe harbor.

The availability of defenses in civil suits that are unavailable in criminal prosecutions runs counter to common sense. At first glance, it seems unfair that a filesharing service could be criminally prosecuted for acts that do not warrant civil liability. Indeed, the preeminent copyright treatise, *Nimmer on Copyright*, has even declared such a prosecution impossible: “Conduct that does not give rise to civil liability for copyright infringement cannot constitute criminal infringement either.”<sup>116</sup> But an examination of these defenses demonstrates why they are inapplicable to criminal cases—and why this should not be troubling.

The first defense applicable only to civil actions is failure to register a work. Although Congress no longer requires registration before copyright protection applies, no civil action may be brought (except for rights of attribution) until a work has been registered.<sup>117</sup> But the statute instituting this limitation says nothing of criminal sanctions, and this was no drafting error. Congress intentionally eliminated the registration hurdle in criminal cases through the 2008 PRO-IP Act,<sup>118</sup> making it easier to enforce copyright criminally than civilly. Congress’s reasoning, as memorialized in the house report corresponding to the PRO-IP Act, was that the blameworthiness of infringement does not depend upon registration, because “[t]he lack of a registration does not make the

---

<sup>116</sup> 4 NIMMER & NIMMER, *supra* note 35, at § 15.01(A)(2).

<sup>117</sup> 17 U.S.C. § 411(a) (2012) (“[N]o civil action for infringement of the copyright in any United States work shall be instituted until preregistration or registration of the copyright claim has been made in accordance with this title.”).

<sup>118</sup> Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub. L. No. 110–403, 122 Stat. 4256; *see also* 17 U.S.C. § 411(a); 4 NIMMER & NIMMER, *supra* note 35, at § 15.07. Before the amendment, it was an open question whether § 411 applied to criminal and civil actions. *See* Michael M. DuBose, *Criminal Enforcement of Intellectual Property Laws in the Twenty-First Century*, 29 COLUM. J.L. & ARTS 481, 488 (2006) (“[W]hether or not the term ‘action’ in § 411 includes criminal prosecutions is a highly relevant question for today’s prosecutors. Unfortunately, there is no reported decision addressing the issue in the context of the current copyright statutes.”).

criminal activity any less egregious.”<sup>119</sup> But that rationale applies with equal force to civil actions; as an explanation, it is incomplete.

One piece of a more complete answer is that criminal enforcement is aimed at infringement that may never be the subject of civil actions. For example, foreign works do not have to register to obtain copyright protection, but the government would still want to police against their infringement.<sup>120</sup> And criminal infringement can involve a slew of different works, some registered, some not. Many works carry a pre-registration problem. A draft memoir,<sup>121</sup> or early cut of an anticipated movie,<sup>122</sup> or even works never intended for publication at all<sup>123</sup> may be particularly attractive to infringers despite their unregistered status. Also, criminal infringers might copy many works—think mass production of DVDs—and the government’s interest in punishing that infringement does not vary when some works are registered and others are not.

That last point is the most crucial: The public has a different interest in criminal prosecution than an author has in civil enforcement. The desire to enforce obedience to the laws is very different than an author’s desire for compensation for their works. Given the benefits of copyright law to authors, requiring authors to take the beneficial step of registering their works before they can

---

<sup>119</sup> H.R. Rep. No. 110–617, at 23 (2008).

<sup>120</sup> See Tyler T. Ochoa, *Is the Copyright Public Domain Irrevocable? An Introduction to Golan v. Holder*, 64 VAND. L. REV. EN BANC 123, 127–28 (2011) (discussing enforcement of copyright for foreign works).

<sup>121</sup> See, e.g., *Harper & Row, Publishers, Inc. v. Nation Enter’s*, 471 U.S. 539, 547–48 (1985) (holding registration of President Ford’s memoir required for civil suit, though it had not yet been published, when news magazine copied key excerpts).

<sup>122</sup> To address this problem for the movie industry, Congress created a preregistration regime in 17 U.S.C. § 408(f) (2012) to preserve a right to statutory damages when an unpublished (and incomplete) work has been infringed. See *Sleep Sci. Partners v. Lieberman*, 09-04200 CW, 2010 WL 1881770, at 6 (N.D. Cal. May 10, 2010) (noting that Congress, in enacting preregistration, was “concerned, in large part, with the piracy of movies”).

<sup>123</sup> See, e.g., *Salinger v. Random House, Inc.*, 811 F.2d 90, 93 (2d. Cir. 1987) (noting that author was forced to register copyright in unpublished letters to prevent their publication), *supplemented on denial of reh’g*, 818 F.2d 252 (2d Cir. 1987).

reap these benefits is equitable and efficient. But no interest is served in requiring the government to persuade rights-holders to register their works before prosecuting criminals. The attachment of copyright at the moment of creation—not the moment of registration—would be a fiction if enforcement of copyright were impossible absent registration.

As a practical matter, however, most criminal prosecutions will focus on infringement of registered works.<sup>124</sup> This is especially so because an element of infringement is that the work used be under copyright of another,<sup>125</sup> and registration is the most expeditious way to prove a valid copyright.<sup>126</sup> While the author's failure to register copyright is not a defense against criminal prosecution, it is a means to cast doubt upon authorship.

The second defense applicable only to civil actions is the safe harbor of the DMCA. That provision shields Internet service providers like Megaupload from suits for "monetary relief, or . . . injunctive or other equitable relief."<sup>127</sup> The provision says nothing about criminal sanctions. Much ink has been spilled speculating about the effect of that omission and whether Megaupload will attempt to use the DMCA's safe harbor as a defense against the Department of Justice.<sup>128</sup>

As it turns out, the safe harbor is a red herring.<sup>129</sup> Despite concerns expressed by observers,<sup>130</sup> the DMCA's safe harbor

---

<sup>124</sup> 4 NIMMER & NIMMER, *supra* note 35, at § 15.01(A)(2).

<sup>125</sup> 17 U.S.C. § 501(a) (2012), *invalidated on other grounds by* Nat'l Ass'n of Bds. of Pharmacy v. Bd. of Regents of the Univ. Sys. of Ga., 633 F.3d 1297 (11th Cir. 2011).

<sup>126</sup> *See* 17 U.S.C. § 410(c) (2012) ("In any judicial proceedings the certificate of a registration . . . shall constitute prima facie evidence of the validity of the copyright . . .").

<sup>127</sup> 17 U.S.C. § 512(c) (2012).

<sup>128</sup> *See, e.g.,* Graeber, *supra* note 1, at 193.

<sup>129</sup> The use of "red herring" to mean a diversion or false trail likely originated from a tale by Michael Quinion, who trained his dogs to hunt by dragging a "red" herring (so called because the smoking and salting process turned the meat red) behind him; red herrings were known to be especially pungent, and the scent would have been easy for a dog to follow. *See* 11 WILLIAM COBBETT ET AL., COBBETT'S POLITICAL REGISTER 232 (London 1807). The idiomatic use of "red herring" to mean a false trail became a recurring joke in *A Pup Named*

provision will not feature prominently in the Megaupload prosecution, nor any other. To understand why, keep in mind that the safe harbor provision (the particular one for which most filesharing services are eligible, as there are several in the DMCA) has three elements: (1) lack of knowledge or awareness of infringement; (2) lack of financial benefit from infringement under defendant's control; and (3) expeditious response to requests to remove infringing material.<sup>131</sup> The common parlance for the third element is "notice and takedown,"<sup>132</sup> and several companies—such as YouTube—have successfully defended against civil suits in part by demonstrating their notice and takedown compliance.<sup>133</sup> But the popular focus on the third element, the expeditious compliance

---

*Scooby-Doo*, as the crime-solving dog and his friends always suspected a ne'er-do-well named "Red Herring." See, e.g., ABC television broadcast, *A Pup Named Scooby-Doo: A Bicycle Built for Boo!* (Sept. 10, 1988).

<sup>130</sup> See Mantel, *supra* note 17, at 98.

<sup>131</sup> The relevant statute provides:

(c) Information residing on systems or networks at direction of users.--

(1) In general.--A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider--

(A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

17 U.S.C. § 512(c) (2012).

<sup>132</sup> See, e.g., *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 27 (2d Cir. 2012) (explaining notification "commonly known as a 'takedown notice'").

<sup>133</sup> See, e.g., *Perfect 10, Inc. v. Google, Inc.*, 653 F.3d 976, 980–82 (9th Cir. 2011); see also *supra* Part III (discussing the YouTube case).

with notice and takedown, neglects the first: lack of knowledge or awareness of infringement. This is a subset of the first element of a criminal prosecution: willfulness.

In fact, the willfulness requirement provides even more protection than the DMCA's safe harbor. Courts have disagreed about exactly what constitutes "willful" infringement, but at a minimum the infringer must *know* that they are copying or performing a work (or in cases of secondary liability, aiding and abetting others in copying or performing).<sup>134</sup> Because willful infringement cannot be done without knowledge or awareness of infringement, anyone who satisfied the first element of DMCA's safe harbor would have already defeated a criminal prosecution.<sup>135</sup> But if a site's owners *are* aware of infringing files, no matter how quickly they comply with notice and takedown requests, they cannot take advantage of the safe harbor provision. Yet these owners with knowledge might be able to defeat a criminal prosecution if they can prove that they were ignorant of their infringement, despite knowing their actions; i.e., that they were not "willful."

The most famous example of intentional but still-innocent infringement is that of Dennis Moran, a mom-and-pop video rental storeowner and police officer.<sup>136</sup> The FBI arrested Moran for making a single copy of "Crocodile Dundee II," amongst other movies, and then renting the copies in lieu of the originals.<sup>137</sup> When federal agents arrived, Moran led them directly to the originals of the copied movies and told the agents exactly what he'd been doing. He believed his copying was perfectly legal, so long as he made only one copy of each video cassette. In a bench trial, the judge acquitted Moran, finding that his infringement was not "willful." Moran was unsophisticated, cooperated with police, and purchased multiple copies of the same movie rather than make more than one copy of each video.<sup>138</sup> Although Moran shifted the risk of loss for each video from himself to the copyright owner, he

---

<sup>134</sup> See 4 NIMMER & NIMMER, *supra* note 35, at § 15.01.

<sup>135</sup> See, e.g., Graeber, *supra* note 1, at 193.

<sup>136</sup> United States v. Moran, 757 F. Supp. 1046 (D. Neb. 1991).

<sup>137</sup> *Id.* at 1047.

<sup>138</sup> *Id.* at 1052.

believed, erroneously but honestly, that this was a permitted fair use.<sup>139</sup>

The *Moran* case has inspired what this Article terms the “Tinker Bell defense.”<sup>140</sup> If people *believe* that their actions do not violate copyright laws, they can never be convicted of criminal copyright infringement. That argument has become an unfortunate darling of legal academia.<sup>141</sup> This argument represents a case of literal wishful thinking—but opponents to criminal copyright cannot wish the law away.

There is a crucial difference between someone who does not know that his actions are wrong, like *Moran*, and someone who knows his actions are wrong but believes that he has found a gap in the law that he can exploit. The latter constitutes willfulness even if honestly believed. For example, a recurring argument raised by *pro se* criminal defendants is that the statute giving federal district courts original jurisdiction in criminal cases, 18 U.S.C. § 3231 (2012), was improperly enacted and thus all federal criminal prosecutions are illegal. That argument has been thoroughly

---

<sup>139</sup> *Id.* *Moran* is an extreme case and represents the most stringent willfulness standard applied in a criminal context. See 5 NIMMER & NIMMER, *supra* note 35, at § 15.01(2). Other courts have held that infringement is willful when the infringer intends their actions, even if the defendant erroneously believes their acts are not infringing. *Id.*; see, e.g., *United States v. Backer*, 134 F.2d 533 (2d Cir. 1943).

<sup>140</sup> Tinker Bell is a fairy from the children’s play “*Peter Pan*.” In the play, Tinker Bell (portrayed as a bright spot of light) drinks poison meant for Peter, saving his life. The fairy nearly succumbs to the deadly poison, but tells the audience (through Peter, the only one who can understand her speech, which is depicted as tinkling bells) that she will get better “if children believe in fairies.” Peter urges the audience, “Do you believe in fairies? . . . If you believe, clap your hands!” See J.M. BARRIE, *PETER PAN*, act 4 (1904). The audience’s applause then revives Tinker Bell. See *id.*

<sup>141</sup> See, e.g., Eric Goldman, *Comments on the Megaupload Prosecution (a Long-Delayed Linkwrap)*, TECH. & MARKETING L. BLOG (Apr. 30, 2012), <http://blog.ericgoldman.org/archives/2012/04/megaupload.htm> (“Megaupload’s business choices may not have been ideal, but Megaupload has a number of strong potential defenses for its users’ activities, including 512(c), lack of volitional conduct and more. Whether it actually qualified for these is irrelevant; Megaupload’s subjective belief in these defenses should destroy the willfulness requirement.”).

discredited,<sup>142</sup> but many defendants, nonetheless, honestly believe it—should that belief defeat the “willfulness” requirement in criminal copyright cases?

The answer must be “No.” The willfulness requirement exists to protect the accidental infringer, not the Holmesian “bad man.”<sup>143</sup> After all, the “bad man” is motivated to learn the law only in order to avoid entanglement with it; were he told that by dint of his own belief he could render himself immune to prosecution, he would never learn the law at all, or learn it wrong on purpose, and certainly never obey it unless it suited him.<sup>144</sup> That cannot be right. Instead, defendants who knowingly aid or abet the infringement of copyright are not any less “willful” for believing that a flaw in the statute protects them. And a filesharing service that knows its users are infringing upon copyrighted works but erroneously believes that it may qualify for the DMCA safe harbor by taking down infringing videos and then reposting them is just as “willful” as a defendant who intentionally commits a crime but believes that no court will have jurisdiction to try him.

In Megaupload’s case, its strongest defense against the charges may indeed be a lack of willfulness—if Megaupload honestly believed that it was effectively policing against infringing content—then it is not guilty of aiding and abetting criminal

---

<sup>142</sup> See, e.g., *Mims v. United States*, No. 9:06CV166, 2006 WL 2559534 (E.D. Tex. Sept. 1, 2006); *Derleth v. United States*, No. L-05-205, 2006 WL 1804618 (S.D. Tex. June 27, 2006); *United States v. Risquet*, 426 F. Supp. 2d 310 (E.D. Pa. 2006); *Jones v. Unknown Warden*, No. 4:06CV00082 (ERW), 2006 WL 389833 (E.D. Mo. Feb. 17, 2006); *United States v. Lawrence*, No. 02 CR 200, 2006 WL 250702 (N.D. Ill. Jan. 27, 2006).

<sup>143</sup> Oliver Wendell Holmes, *The Path of the Law*, 10 HARV. L. REV. 457, 459 (1897) (“[A] bad man has as much reason as a good one for wishing to avoid an encounter with the public force, and therefore you can see the practical importance of the distinction between morality and law. A man who cares nothing for an ethical rule which is believed and practised by his neighbors is likely nevertheless to care a good deal to avoid being made to pay money, and will want to keep out of jail if he can.”).

<sup>144</sup> See *id.* (“If you want to know the law and nothing else, you must look at it as a bad man, who cares only for the material consequences which such knowledge enables him to predict, not as a good one, who finds his reasons for conduct, whether inside the law or outside of it, in the vaguer sanctions of conscience.”).

copyright infringement. Commentaters argue that Megaupload's "subjective belief" that it complied with the safe harbor provision will defeat the willfulness requirement,<sup>145</sup> but as discussed earlier, if Megaupload fails to qualify for the safe harbor, it will be because the government proves that Megaupload knew about the infringing content (and if the government does not, Megaupload will surely be acquitted of the aiding and abetting charge). The mistaken belief that one is immune from prosecution for aiding and abetting conduct one *knows* is illegal does not disprove willfulness.

For the reason stated above, if the facts alleged in the indictment are proved, the willfulness requirement will likely be met. According to the indictment, the operators of Megaupload were just as intentional in their copyright infringement as The Pirate Bay, collecting advertising revenues generated by infringing content and exchanging incriminating emails showing that they knew about the infringement on their service.<sup>146</sup> One operator joked to another that they "have a funny business . . . modern days pirates :)," to which his co-conspirator responded, "we're not pirates, we're just providing shipping services to pirates :)." <sup>147</sup> Megaupload similarly sold premium access to unlimited streaming of uploaded content and financially rewarded users—even those

---

<sup>145</sup> See, e.g., Goldman, *supra* note 141 ("Megaupload's subjective belief in these defenses should destroy the willfulness requirement.").

<sup>146</sup> See Indictment, *supra* note 80, at 3, 42.

<sup>147</sup> *Id.* at 42. In another exchange, Kim Dotcom sent an employee an email from a broadband service provider, which had complained that its users were having trouble downloading content from Megaupload.com. *Id.* The indictment says that the screenshots in the email appeared to be an ongoing download of an episode of the television series "The Simpsons" entitled "Treehouse of Horror XIII." *Id.* Unfortunately, Megaupload failed to learn that episode's moral about the dangers of unauthorized copying. See *id.* In the segment "Send in the Clones," Homer (the patriarch of the eponymous family) buys a hammock with a terrible curse: It clones anyone who uses it. *The Simpsons: Treehouse of Horror XIII, "Send in the Clones"* (FOX Television Broadcast, 2002). Homer clones himself several times, but finds that the cloned Homers get him into trouble. *Id.* He abandons them and the hammock in a distant town, but the clones begin some unauthorized copying of their own, making an army of Homer clones that overrun Springfield. *Id.* Copyright infringers, take note: When the federal government gets involved at the segment's end, things end badly for the unauthorized copiers. See *id.*



previously caught uploading infringing material—for uploading popular content and for posting links to that same content on other websites.<sup>148</sup> This practice not only increased traffic but also allowed Megaupload to avoid listing infringing videos directly on the site, concealing the scope of the infringing content on its servers.<sup>149</sup> To rebut claims of infringement, Megaupload had instituted an “Abuse Tool,” allowing copyright holders to report, and purportedly remove, infringing content. But the indictment alleges that the company received millions of requests to remove infringing content and, “at best, only deleted the particular URL of which the copyright holder complained, and purposefully left the actual infringing copy of the copyrighted work on the Mega Conspiracy-controlled server and allowed access to the infringing work to continue.”<sup>150</sup>

If these allegations are true, Megaupload is likely subject to not only criminal but civil liability, as well. And, in fact, the company was sued by pornography company Perfect 10 even before the Department of Justice stepped in.<sup>151</sup> The case brought by Perfect 10, however, was short-lived. It settled early in the proceeding after the district court denied Megaupload’s motion to dismiss.<sup>152</sup> The court reasoned that, if the plaintiff’s allegations were true, any lack of knowledge on Megaupload’s part about the infringement on its site was willful blindness.<sup>153</sup>

---

<sup>148</sup> Indictment, *supra* note 80, at 6–7, 32–33.

<sup>149</sup> *Id.* at 6–7.

<sup>150</sup> *Id.* at 10–11.

<sup>151</sup> Perfect 10, Inc. v. Megaupload, Ltd., No. 3:11-cv-00191, ECF Doc. 16, at 9 (S.D. Cal. July 26, 2011).

<sup>152</sup> Perfect 10, Inc. v. Megaupload, Ltd., No. 3:11-cv-00191, ECF Doc. 27 (S.D. Cal. Oct. 18, 2011) (dismissing case with prejudice under FED. R. CIV. P. 41(a)(1)).

<sup>153</sup> *Id.* Because Megaupload settled the lawsuit, it probably cannot seek contribution from any users who may have been the direct infringers, even if it faced only secondary liability. See, e.g., Jeremiah Newhall, *Claims for Contribution Against Nonsettling Co-Tortfeasors*, 26 C.B.A. REC., no.5, at 40–41 (2012). Since the prosecution, two music companies have sought millions in damages from Megaupload, but their suit is stayed pending further developments in the criminal case. Jeremy Kirk, *Megaupload Files Motion to Delay Civil Suit*, PCWORLD, (May 10, 2012, 6:20 PM), [http://www.pcworld.com/article/255423/megaupload\\_files\\_motion\\_to\\_delay\\_ci](http://www.pcworld.com/article/255423/megaupload_files_motion_to_delay_ci)

## V. RULES OF ENGAGEMENT: WHEN CRIMINAL PROSECUTION IS WARRANTED

Even with the high bar of willfulness, there are almost certainly more filesharing services subject to criminal liability than can be prosecuted. Since the time filesharing services first became mainstream, technological developments have made them easier to create, and millions of people have shown themselves willing to skirt the law to share music online.<sup>154</sup> Consider, for instance, that a 2011 study concluded that, in the United States alone, “17.53% of Internet traffic was estimated to be infringing,” excluding pornography.<sup>155</sup> Yet in 2012, the Department of Justice received only 79 investigative matters related to copyright infringement of any kind under 18 U.S.C. § 2319 (2012) and filed only 40 cases against 59 defendants.<sup>156</sup>

---

vil\_suit.html; *Microhits, Inc. v. Megaupload, Ltd.*, No. 1:12-cv-00327, ECF Doc. 36 (E.D. Va. June 15, 2012) (denying plaintiff’s motion to reconsider an earlier-imposed stay). Interestingly, it was actually Megaupload that was the more aggressive litigator, suing Universal Music Group for allegedly unlawfully removing from YouTube a video showcasing music stars endorsing Megaupload. Eriq Gardner, *Megaupload Drops Lawsuit Against Universal Music Over Viral Video (Exclusive)*, THE HOLLYWOOD REPORTER (Jan. 21, 2012, 10:18 AM), <http://www.hollywoodreporter.com/thr-esq/megaupload-universal-music-group-lawsuit-dropped-283767>. This lawsuit was dismissed without prejudice in January 2012. *Id.* The video featured endorsements from artists William Adams (“will.i.am”), Jamie Foxx, Kanye West, Sean Combs (“Diddy”), Jonathan Smith (“Lil Jon”), Chris Brown, and professional celebrity Kim Kardashian. OKFocus, *MEGA UPLOAD SONG!!!! HTTP://OKFOC.US*, VIMEO (Dec. 9, 2011), <http://vimeo.com/33424808>.

<sup>154</sup> See ANDERSON, *supra* note 5, at 191, 201. These concerns lead to what journalist Nate Anderson calls the “unique scale problem” posed by copyright since the creation of the Internet. *Id.* at 191. Anderson suggests, however, that the government may be the “one entity” with “the brawn to force Internet providers to take action against their users.” *Id.* at 207.

<sup>155</sup> ENVISIONAL LTD., AN ESTIMATE OF INFRINGING USE ON THE INTERNET 3 (2011), *available at* [http://documents.envisional.com/docs/Envisional-Internet\\_Usage-Jan2011.pdf](http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf). Why exclude pornography? The infringing status can be “difficult to discern.” *Id.* at 2.

<sup>156</sup> See U.S. DEP’T OF JUSTICE, FY 2012 PERFORMANCE AND ACCOUNTABILITY REPORT app. D, at D-3 (2013) [hereinafter 2012 ACCOUNTABILITY REPORT]. The trend has been similar in years past: In 2011, of 82 investigative matters, only 46 cases were filed; in 2010, it was 74 cases out of 132. See U.S. DEP’T OF

Any potential increase in criminal copyright enforcement, however, faces unique challenges even aside from proving a case, for two reasons. First, anti-copyright advocates can be a vocal group in the United States, ready to incite public backlash. Megaupload, for example, garnered the support of important Internet personalities ranging from respected entrepreneur Steve Wozniak,<sup>157</sup> co-founder of Apple Computers, to the notorious hacker group Anonymous,<sup>158</sup> which mounted attacks following the

---

JUSTICE, FY 2011 PERFORMANCE AND ACCOUNTABILITY REPORT app. D, at D-3 (2012); U.S. DEP'T OF JUSTICE, FY 2010 PERFORMANCE AND ACCOUNTABILITY REPORT app. E, at E-3 (2011). This data includes *all* types of copyright infringers, not just Internet infringers. See 2012 ACCOUNTABILITY REPORT at D-1.

<sup>157</sup> Aaron Souppouris, *Steve Wozniak Speaks Out In Favor of Net Neutrality, Supports Megaupload*, THE VERGE (June 27, 2012, 8:02 AM), <http://www.theverge.com/2012/6/27/3120355/steve-wozniak-net-neutrality-megaupload-support>.

<sup>158</sup> More deserves to be said about the “group” Anonymous, which has its origins in a copyright dispute with the Church of Scientology. Simply put, there is no evidence of a capital-A “anonymous” entity, but only of anonymous individuals who commit acts ascribed to “Anonymous.” There is little or no evidence of central coordination or that most of the purported “members” know, or even agree with, one another. In this sense, it is more akin to a mass movement, à la the Occupy Wall Street protests. The Anonymous legend appears to have its origins in a report by a local news team for the Los Angeles Fox television affiliate, which described “a hacker group called Anonymous.” But as online magazine Wired explained, “Fox 11 actually stumbled across the /b/ (NSFW) channel of 4chan” (or possibly 420chan) an “image sharing and posting site where every poster posts as Anonymous. Here, supremely bored 15-year olds post obscene pictures and stupid photo-shopped images for others to comment on. They also randomly swarm and try to overwhelm online sites and forums they consider annoying.” See Ryan Singel, *Investigative Report Reveals Hackers Terrorize the Internet for LULZ*, WIRED (July 27, 2007, 3:54 PM), <http://www.wired.com/threatlevel/2007/07/investigative-r/>. The first instance of anyone publicly claiming to act for “Anonymous” as a group came in the form of a press release posted (anonymously) through free press-release generator PRlog.org, and heralding a denial-of-service attack against the Church of Scientology in January 2008. *Internet Group Anonymous Declares “War on Scientology,”* PRLOG (Jan. 21, 2008), <http://www.prlog.org/10046797-internet-group-anonymous-declares-war-on-scientology.html>. The author of the press release found the church’s use of copyright to prevent publication and criticism of its teachings to be objectionable, especially when the church issued takedown notices to web sites hosting a video of a Tom Cruise interview about the church.

indictment that briefly disabled several government and music-industry websites.<sup>159</sup> Second, it is very difficult to prosecute infringers who often live outside of the United States and operate conspiracies that span across the globe. Barely 10% of Internet users are in the United States,<sup>160</sup> and many Internet service providers have spread their operations across multiple jurisdictions, as Megaupload did: The company was based in Hong Kong, but had servers in the United States and elsewhere, and its operators were captured in both Europe and New Zealand.<sup>161</sup>

Given these challenges, prosecutors should save their powder for when criminal prosecution is most necessary, rather than firing

---

*Id.* Shortly thereafter, a number of protests against the church arose, at which people wore Guy Fawkes masks based on the mask worn by protagonist “V” in the graphic novel and film “V for Vendetta,” in which a masked terrorist blows up Parliament and inspires a horde of imitators. See generally ALAN MOORE AND DAVID LLOYD, *V FOR VENDETTA* (DC Comics 1982) (depicting a mysterious masked revolutionary who calls himself “V” and works to destroy the totalitarian government in a post-nuclear UK); *V FOR VENDETTA* (Warner Bros. 2005) (adapting the 1982 graphic novel for the screen).

<sup>159</sup> Josh Halliday, *Anonymous Launches Attacks in Wake of Megaupload Closure*, THE GUARDIAN (Jan. 20, 2012, 8:52 AM), <http://www.guardian.co.uk/technology/2012/jan/20/anonymous-attacks-after-megauploads-closure>.

Recently, open-information activists have turned their attention to Aaron Swartz, who committed suicide in the midst of federal prosecution for his role in obtaining academic articles from the online database JSTOR that he apparently planned to distribute for free. Caroline Bankoff, *Aaron Swartz’s Suicide Spurs Outrage at Prosecutors*, N.Y. MAGAZINE (Jan. 13, 2013, 2:00 PM), <http://nymag.com/daily/intelligencer/2013/01/swartzs-suicide-spurs-outrage-at-prosecutors.html>.

<sup>160</sup> *Internet Users – Top 20 Countries – Internet Usage*, INTERNET WORLD STATS, <http://www.internetworldstats.com/top20.htm> (last updated Mar. 6, 2013).

<sup>161</sup> Nick Perry, *Popular File-sharing Website Megaupload Shut Down*, USATODAY.COM (Jan. 20, 2012, 1:00 PM), <http://usatoday30.usatoday.com/tech/news/story/2012-01-19/megaupload-feds-shutdown/52678528/1>

(describing the company as “based in Hong Kong”). As a reporter who visited Dotcom after the indictment noted, the Megaupload conspirators made their homes all over the globe: “Andrus Nomm, a resident of both Turkey and Estonia, was captured in Holland; Sven Echternach escaped to his home in Germany (which does not extradite its citizens); and Julius Bencko of Slovakia remains at large. The other three were, like Kim, nabbed in New Zealand.” Graeber, *supra* note 1.

at will whenever an infringing website comes within their jurisdiction. This suggestion of prosecutorial discretion, however, requires a brief discussion of the limits of that discretion before turning to specific guidelines for enforcement of copyright law.

#### A. *The Limits of Prosecutorial Discretion*

Federal prosecutors were once afforded significant discretion in deciding whether to bring charges against alleged criminals.<sup>162</sup> But beginning in 2003 Attorney General John Ashcroft amended the rules to create a straightforward approach to prosecutorial discretion; there wasn't any.<sup>163</sup> United States Attorneys were required to "charge and pursue the most serious, readily provable offense or

---

<sup>162</sup> Michael A. Caves, *The Prosecutor's Dilemma: Obligatory Charging Under the Ashcroft Memo*, 9 J. L. & SOC. CHALLENGES 1, 1 (2008) ("Prior to former-Attorney General Ashcroft's Memo, federal prosecutors were afforded wide discretion when deciding whether to charge a suspect with a crime because of the significant impact that criminal charges can have on a suspect.").

<sup>163</sup> Memorandum from John Ashcroft to all federal prosecutors (Sept. 22, 2003), available at [http://www.usdoj.gov/opa/pr/2003/September/03\\_ag\\_516.htm](http://www.usdoj.gov/opa/pr/2003/September/03_ag_516.htm); see also Caves, *supra* note 162, at 2 ("After then-Attorney General John Ashcroft's memo, federal prosecutors were required to charge the most serious, readily provable offense supported by the facts of the case, without regard for any overarching notions of justice."). We slightly overstate the reality. The memo could not eliminate prosecutorial discretion as completely as it intended: it still remained for the U.S. Attorney to decide whether an offense was "supported by the facts of the case," an objective standard, but one pliable enough that a sympathetic prosecutor could decline to pursue charges in an extreme case. Consider the hypothetical of John McClane, a New York City police officer who, while visiting his estranged wife at her office's holiday party in Los Angeles's Nakatomi Plaza, encounters a group of international terrorists who take his wife and her work colleagues hostage. See *DIE HARD* (20th Century Fox 1988). McClane knows that he is not allowed to possess a machine gun. See 18 U.S.C. § 922(o) (2012); see also *United States v. Rybar*, 103 F.3d 273, 283 (3d Cir. 1996) (Slovitar, C.J.) (upholding the constitutionality of 18 U.S.C. § 922(o)). Nonetheless McClane kills a terrorist, takes his machine gun, and rescues his wife and all of the hostages (except for Harry Ellis). See *DIE HARD*. A U.S. Attorney would be obliged to prosecute McClane under this policy, but might nonetheless decline to prosecute, arguing (implausibly) that the charge of possession of a machine gun was not "supported by the facts of the case." Of course, McClane has a very plausible defense of necessity, but the elements of the charge are nonetheless present.

offenses that are supported by the facts of the case.”<sup>164</sup> This kind of strict adherence to the letter of the law calls to mind Inspector Javert’s pursuit of Jean Valjean. It springs from a philosophy of legal fidelity that regards prosecutorial discretion as antidemocratic. Under this view, Congress enacts the law according to the will of the people, and appointed judges and prosecutors should stringently enforce those laws.<sup>165</sup> If the law is unjust, its rigid enforcement will force the Congress to amend it; making exceptions would only permit unjust laws to linger on the books. This approach has the added benefit of uniformity. The elimination of discretion admits no space for discrimination; it is truly blind to the accused’s color, race, gender, or creed.<sup>166</sup>

But indiscriminate prosecution is also inefficient. A criminal code that accounted for every eventuality would be too cumbersome to administer. Even now, the United States Code is far too voluminous for any person to know all the laws that they are obliged to obey, and it grows each year.<sup>167</sup> Prosecutorial discretion, by contrast, is both more efficient and more just.<sup>168</sup>

---

<sup>164</sup> Ashcroft, *supra* note 163.

<sup>165</sup> See Erik Luna, *Principled Enforcement of Penal Codes*, 4 BUFF. CRIM. L. REV. 515, 534 (2000) (“One historic definition of the rule of law argues that discretionary power has no place in legitimate government.”); Jeffrey Reiman, *Is Police Discretion Justified in a Free Society?*, in *HANDLED WITH DISCRETION: ETHICAL ISSUES IN POLICE DECISION MAKING* 71, 81–82 (John Kleinig ed., 1996) (“The laws should express the actual treatment that the society wants, and police enforcement of those laws should be as automatic as possible. The reduction of discretion should be carried throughout the system.”).

<sup>166</sup> Indeed, uniformity was a key concern raised in the Ashcroft memorandum, which concludes, “Fundamental fairness requires that all defendants prosecuted in the federal criminal justice system be subject to the same standards and treated in a consistent manner.” Ashcroft, *supra* note 163.

<sup>167</sup> See Gene Healy, *Introduction*, in *GO DIRECTLY TO JAIL: THE CRIMINALIZATION OF ALMOST EVERYTHING* vii (Gene Healy ed., 2004) (maintaining that, as a result of the increase in federal crimes, listed throughout the U.S. Code and incorporating violations of federal regulations, “even teams of legal researchers—let alone ordinary citizens—cannot reliably ascertain what federal law prohibits”).

<sup>168</sup> See generally Amie N. Ely, Note, *Prosecutorial Discretion as an Ethical Necessity: The Ashcroft Memorandum’s Curtailment of the Prosecutor’s Duty to “Seek Justice,”* 90 CORNELL L. REV. 237, 277–78 (2004) (arguing that the Ashcroft memorandum inappropriately constrained prosecutorial discretion).

Rather than requiring Congress to codify every exception to criminal liability, Congress can criminalize a broad category of usually blameworthy conduct—widespread copying of protected works, for example—alongside a range of punishments. The people then trust prosecutors to discern which infringement is truly reprehensible, and trust judges to punish the condemned copiers according to their culpability. Although this method admits the human frailties of prejudice and discrimination, it also fosters the virtue of mercy.<sup>169</sup>

The restoration of prosecutorial discretion in the United States Attorneys' offices in 2010<sup>170</sup> thus came as a welcome change. The Attorney General now regards prosecutorial discretion as “essential to the fair, effective, and even-handed administration of the federal criminal laws.”<sup>171</sup> Accordingly, each office of the United States Attorney must maintain its own written guidelines for the exercise of discretion.<sup>172</sup>

More recently, Attorney General Eric Holder announced an even more aggressively lenient use of prosecutorial discretion.<sup>173</sup> At Holder's direction, the Justice Department issued new guidelines dubbed *Smart on Crime*, which aim at reducing the

---

<sup>169</sup> Appropriate prosecutorial discretion also guards against a situation in which, as Harvey Silverglate vividly puts it, “the federal criminal justice system has become a crude conviction machine instead of an engine of truth and justice.” HARVEY A. SILVERGLATE, *THREE FELONIES A DAY: HOW THE FEDS TARGET THE INNOCENT* lxvi (Large Print ed. 2010).

<sup>170</sup> Memorandum from Eric H. Holder, Jr. to all federal prosecutors (May 19, 2010), available at <http://edca.typepad.com/files/holder-memo-re-charging-and-sentencing-decisions-1.pdf>.

<sup>171</sup> *Id.*

<sup>172</sup> *Id.*

<sup>173</sup> See U.S. Dep't of Justice, *Attorney General Eric Holder Delivers Remarks at the Annual Meeting of the American Bar Association's House of Delegates*, JUSTICE.GOV (Aug. 12, 2013), <http://www.justice.gov/iso/opa/ag/speeches/2013/ag-speech-130812.html> (announcing a modification of the Justice Department's charging policies to avoid mandatory minimum sentences for low-level, nonviolent drug offenders and arguing that “federal prosecutors cannot—and should not—bring every case or charge every defendant who stands accused of violating federal law”).

sentences for nonviolent drug crimes.<sup>174</sup> Citing the enormous costs to the government of a burgeoning population of aging, nonviolent federal prisoners, the memo instructs federal prosecutors *not* to charge the most serious, readily provable offense against nonviolent drug offenders.<sup>175</sup> Instead, prosecutors are to omit specific drug quantities, so that judges will not be bound by mandatory minimum sentences that the Attorney General considers both draconian and expensive.<sup>176</sup> Like simple drug possession, criminal copyright infringement is a nonviolent offense, and the following guidelines aim to similarly limit the needless expense of housing harmless prisoners.

*B. Guidelines for Criminal Copyright Enforcement Against Filesharing Services*

In light of prosecutors' discretion to enforcement copyright law, this Article proposes three guidelines to shape that discretion. These suggestions are not intended as rules—that would be anathema to the independent discretion the guidelines should foster. But wholly untethered discretion leads to unpredictable results; it prevents the Holmesian “bad man” from knowing the price of his transgressions.

First, criminal enforcement of copyright should proceed only on established theories of liability. The importance of this guideline is underscored by the United States Attorneys' Manual on prosecuting copyright cases, which cautions that “unsuccessful prosecution may be counterproductive not only in terms of allocation of resources, but also with respect to deterrence.”<sup>177</sup> Thus, prosecutors are instructed to “carefully evaluate[]” potential legal problems with their case, “particularly with regard to criminal intent.”<sup>178</sup> Additionally, and perhaps more importantly, prosecutors

---

<sup>174</sup> See U.S. DEP'T OF JUSTICE, SMART ON CRIME: REFORMING THE CRIMINAL JUSTICE SYSTEM FOR THE 21ST CENTURY 2–3 (2013), *available at* [http://www.abajournal.com/files/SMART\\_ON\\_CRIME.PDF](http://www.abajournal.com/files/SMART_ON_CRIME.PDF).

<sup>175</sup> *Id.*

<sup>176</sup> *Id.*

<sup>177</sup> UNITED STATES ATTORNEYS' MANUAL § 9-71.010 (2013), [http://www.justice.gov/usao/eousa/foia\\_reading\\_room/usam/title9/71mcrm.htm#9-71.010](http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/71mcrm.htm#9-71.010).

<sup>178</sup> *Id.*



should be hesitant to charge offenses that have not already been clearly defined by civil courts to avoid punishing people before they might reasonably be expected to know that what they're doing is a crime.<sup>179</sup>

As discussed, the theory of secondary liability is established enough to proceed with prosecution against services like Megaupload.<sup>180</sup> Although some critics decry this theory as novel as applied to criminal law,<sup>181</sup> in reality its application is nearly as old as criminal copyright law itself, dating back to 1909 when Congress added the crime of "aiding and abetting" to the Copyright Act to target the theater managers who helped connect traveling infringers to their audiences. In the same way, especially in the wake of *Grokster*, the groundwork has been well-laid for the government to target filesharing services that help infringing

---

<sup>179</sup> In his book *Three Felonies a Day*, Attorney Harvey Silverglate recalls noticing that, as criminal statutes proliferated, "federal prosecutors grew more inclined to bring criminal charges for deeds that, at most, constituted arguable (sometimes barely arguable) civil offenses." SILVERGLATE, *supra* note 169, at liii (emphasis omitted). The questions raised in these criminal cases, he argues, should have been resolved in civil proceedings where "[t]he citizen, if wrong, would have to pay a price measured in dollars; and once the clear meaning of the statute or regulation was established, the citizen would be expected to adhere to it, next time on penalty of criminal indictment and conviction." *Id.*

<sup>180</sup> We caution, however, that, as exemplified by *Flava Works, Inc. v. Gunter*, 689 F.3d 754, 758 (7th Cir. 2012), the liability of "social-bookmarking" and, by that same token, "linking" sites that do not actively encourage infringement is still an evolving area of law. See also *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1169–77 (9th Cir. 2007) (concluding that the adult-entertainment company was unlikely to succeed in claim that Amazon and Google secondarily infringed by displaying thumbnail images of the site's photos as reproduced on infringing sites).

<sup>181</sup> See, e.g., Ross Drath, *Hotfile, Megaupload, and the Future of Copyright on the Internet: What Can Cyberlockers Tell Us About DMCA Reform?*, 12 J. MARSHALL REV. INTELL. PROP. L. 205, 218 (2012) ("The breathtaking indictment alleges criminal secondary infringement, a theory that has not yet been tested in court."); Jennifer Granick, *Megaupload: A Lot Less Guilty Than You Think*, THE CENTER FOR INTERNET AND SOCIETY BLOG (Jan. 26, 2012, 11:47 AM), <http://cyberlaw.stanford.edu/blog/2012/01/megaupload-lot-less-guilty-you-think> ("But the first question from a defense perspective has to be 'Can the Grokster theory of CIVIL liability even be the basis for CRIMINAL copyright claims?' This has never been decided by any Court.").

uploaders reach the global Internet community. As shown by the district court's decisive rejection of Megaupload's motion to dismiss in the *Perfect 10* case,<sup>182</sup> the time is ripe to hold services like Megaupload accountable.

Second, the government should target prominent services. Megaupload is a good example: when indicted, the company claimed to be pulling in 4% of all Internet traffic and averaging 50 million daily visits.<sup>183</sup> This notoriety, or "big fish" factor, is important because many users of filesharing services are low-cost infringers, using search-engines to pirate 99-cent songs or \$10 movies. There are strong odds that shuttering high-traffic websites, those that appear at the top of search queries, will significantly deter these infringers. This theory is bolstered by evidence that, in the wake of Megaupload's shutdown, digital revenues for movie studios increased by 6 to 10%.<sup>184</sup> The company's notoriety appears to have also increased the prosecution's deterrent effect on other services, as seen from a voluntary shutdown of a number of smaller filesharing services following Megaupload's indictment.<sup>185</sup>

Third, criminal copyright enforcement should be limited to circumstances where there is evidence that civil litigation will be futile. The most obvious way that this futility arises is when operators of a filesharing service refuse to respond to civil means of copyright enforcement. This idea is echoed in the U.S. Attorneys' Manual, which recommends that people "who have

---

<sup>182</sup> See *Perfect 10, Inc. v. Megaupload, Ltd.*, No. 11-cv-0191, ECF Doc. No. 16, at 9 (S.D. Cal. July 26, 2011) (denying motion to dismiss in regard to counts of direct and contributory infringement). The case going forward ultimately forced a settlement. *Perfect 10, Inc. v. Megaupload, Ltd.*, No. 3:11-cv-00191, ECF Doc. 27 (S.D. Cal. Oct. 18, 2011).

<sup>183</sup> Indictment, *supra* note 80, at 2–3; see ANDERSON, *supra* note 5, at 222 (referring to Megaupload as "Public Internet Enemy No.1").

<sup>184</sup> See Brett Danaher & Michael D. Smith, *Gone in 60 Seconds: The Impact of the Megaupload Shutdown on Movie Sales* 21 (March 6, 2013) (unpublished manuscript), available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2229349](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2229349).

<sup>185</sup> See, e.g., Drath, *supra* note 181, at 220 ("In the wake of the Megaupload indictment, many important cyberlockers have significantly altered or even shut down their services.").

continued to infringe for financial gain after civil remedies have been successfully invoked should receive particular attention.”<sup>186</sup>

Accordingly, criminal prosecution should be saved for filesharing services demonstrating an egregious disregard for copyright law. Although some services’ scofflaw attitudes may spring from political disdain for copyright protections—The Pirate Bay is affiliated with Sweden’s Pirate Party<sup>187</sup> and Kim Dotcom has publicly disagreed with protections for film releases<sup>188</sup>—opposition to copyright is not a crime. What shows prosecutable contempt for the law are the steps the operators took to scorn takedown complaints and profiteer from blatant infringement. The Pirate Bay operators raked in advertising revenues while publicly ridiculing infringement complaints. Megaupload likewise made millions by selling ads on infringing content<sup>189</sup> while its employees allegedly joked about aiding piracy and dodged takedown requests by reposting links to infringing content. Similarly, after U.S. officials seized TV Shack’s original domain name, the site moved within a day to a new domain, with a front page prominently featuring the cover image of NWA’s rap single “F\*\*\* the Police.”<sup>190</sup> Credible criminal sanctions, including a threat of prison,

---

<sup>186</sup> MANUAL, *supra* note 177, at § 9-71.010.

<sup>187</sup> See Miaoran Li, *The Pirate Party and The Pirate Bay: How the Pirate Bay Influences Sweden and International Copyright Relations*, 21 PACE INT’L L. REV. 281, 289 (2009).

<sup>188</sup> See Adrienne Jeffries, *Pirates Beware: Kim Dotcom’s Mega isn’t the Safe Haven he Says it Is*, THE VERGE (Jan. 31, 2013, 2:30 PM), <http://www.theverge.com/2013/1/31/3933774/kim-dotcoms-new-site-mega-is-a-flop-with-pirates-and-heres-why> (“Dotcom has said publicly that he does not support piracy for music, but does support downloading movies, since the studios force people to wait for staggered releases.”).

<sup>189</sup> According to the indictment, Megaupload made \$25 million in advertising revenues, and an additional \$150 million from selling premium subscriptions. Indictment, *supra* note 80, at 3. Dotcom received more than \$42 million from the conspiracy in 2010 alone. *Id.* at 14.

<sup>190</sup> Christopher Williams, *Student Richard O’Dwyer can be Extradited Over TV Website*, THE GUARDIAN (Jan. 13, 2012, 4:50 PM), available at <http://www.telegraph.co.uk/technology/news/9013803/Student-Richard-ODwyer-can-be-extradited-over-TV-website.html>. The U.S. government seized the new site five months later. Mark Brown, *TVShack creator Richard O’Dwyer’s US extradition*

may be the only effective approach to this type of blatant disregard for the law.

Although potentially necessary, imprisonment of copyright infringers is not ideal. Prison creates a host of societal losses: the expense of running jails, the lockup of wage earners, the potential for civil-rights violations.<sup>191</sup> Moreover, when imprisonment is rarely imposed, as in copyright cases, the deterrent effect is decreased. As Judge Richard Posner has pointed out, “China executes perpetrators of commercial crimes, but very few, and the crimes appear to be rampant.”<sup>192</sup> On the other hand, as David Ladd, former Register of Copyrights, has argued, perhaps “[o]nly criminal penalties, with jail or the prospect of jail, are drastic enough to restrain repeated offenders and to deter the flagrant

---

*appeal delayed*, WIRED.CO.UK (May 30, 2012), <http://www.wired.co.uk/news/archive/2012-05/30/tvshack-appeal-delayed>.

<sup>191</sup> Judge Posner addressed this topic in a recent concurrence from a Seventh Circuit decision affirming a lengthy prison term:

Federal imprisonment is expensive to the government; the average expense of maintaining a federal prisoner for a year is between \$25,000 and \$30,000, . . . and the expense rises steeply with the prisoner’s age because the medical component of a prisoner’s expense will rise with his age, especially if he is still alive in his 70s (not to mention his 80s or 90s). It has been estimated that an elderly prisoner costs the prison system between \$60,000 and \$70,000 a year. . . .

That is not a *net* social cost, because if free these elderly prisoners would in all likelihood receive Medicare and maybe Medicaid benefits to cover their medical expenses. But if freed before they became elderly, and employed, they would have contributed to the Medicare and Medicaid programs through payroll taxes—which is a reminder of an additional social cost of imprisonment: the loss of whatever income the prisoner might lawfully have earned had he been free, income reflecting his contribution to society through lawful employment.

*United States v. Craig*, 703 F.3d 1001, 1003 (7th Cir. 2012) (Posner, J., concurring) (per curiam); see also Richard Posner, *Does America Imprison Too Many People?* Posner, THE POSNER-BECKER BLOG (Dec. 4, 2011, 6:13 PM), <http://www.becker-posner-blog.com/2011/12/does-america-imprison-too-many-people-posner.html> (“[T]he indirect costs of high levels of incarceration must be very great, in the form of the lost output of the large number of prisoners, most of whom are of working age.”).

<sup>192</sup> Richard A. Posner, ANTITRUST LAW 271 (2d ed. 2001). Rather, Judge Posner advocates steeper fines targeted toward deterring specific unwanted activity. *Id.* at 271–73.

kinds of piracy with which Congress has been concerned.”<sup>193</sup> The latter is especially relevant to curbing infringement by companies that can absorb civil penalties as a mere cost of doing business, as Megaupload did with Perfect 10.<sup>194</sup>

The potential for imprisonment is not the only reason why prosecutors might choose to pursue filesharing services through a criminal rather than civil proceeding. In fact, there are at least five procedural benefits to the government in criminal proceedings. Each consequently presents hardships for filesharing services.

First, many of these services are headquartered overseas, making civil litigation against them especially difficult.<sup>195</sup> Interestingly, this problem harkens back to the early reasons for criminal copyright sanctions: the difficulties of enforcing copyright laws against transient performers.<sup>196</sup> Even though extradition for infringers can be difficult to obtain<sup>197</sup>—indeed, the presiding judge in the

---

<sup>193</sup> *Civil and Criminal Enforcement of the Copyright Laws: Hearings Before the Subcomm. on Patents, Copyrights and Trademarks of the S. Comm. on the Judiciary*, 99th Cong. 74 (1985).

<sup>194</sup> Drath, *supra* note 181, at 217.

<sup>195</sup> See Hatch, *International Anti-Piracy Caucus Unveils “2010 International Piracy Watch List,”* HATCH.SENATE.GOV (May 19, 2010), <http://www.hatch.senate.gov/public/index.cfm/releases?ID=b109414b-1b78-be3e-e0b8-34869d0477c4>.

<sup>196</sup> Hardy, *supra* note 25, at 315. As the legislative history of the 1909 amendments to the Copyright Act reveals, the rationale behind the Act’s criminal sanctions were to protect against those infringers who “were both financially irresponsible and transient in their business locations, making injunctions and civil damages futile.” John Lindenberg-Woods, *The Smoking Revolver: Criminal Copyright Infringement*, BULL. COPYRIGHT SOC’Y U.S.A. 63, 66 (1979); see also Harv. L. Rev., *supra* note 26, at 1707.

<sup>197</sup> The U.S. government’s attempts to extradite the operators of Megaupload have so far been unsuccessful. On top of that, Megaupload has twice moved to dismiss the criminal case on the grounds that prosecutors have failed to mail it a copy of the criminal summons as required by Federal Rule of Criminal Procedure 4(c)(3)(C), as the company lacks a “last known address within the district” or a “principal place of business elsewhere in the United States.” Lorraine Bailey, *Feds Scramble to Keep Megaupload in Court*, COURTHOUSE NEWS SERV. (Jan. 16, 2013, 2:16 PM), <http://www.courthousenews.com/2013/01/16/53993.htm>. The fact that the operators are overseas has caused other problems as well. Megaupload’s founder, Kim Dotcom, also challenged the raid on his mansion in a New Zealand court and won: the court found that New

Megaupload case has noted that the defendants “may never be extradited”<sup>198</sup>—it is not even an option in civil litigation.<sup>199</sup> In civil litigation, the best plaintiffs can hope for is that a defendant consents to U.S. jurisdiction or, absent that, that the court might agree to the rare use of Federal Rule of Civil Procedure 4(k)(2) to claim personal jurisdiction over defendants abroad.<sup>200</sup> Even then, if

---

Zealand authorities relied on overbroad—and thus invalid—search warrants and improperly released copies of seized hard drives to the FBI. *Dotcom v. Att’y Gen.* [2012] 3 NZLR 115 (HC) 130–36. The New Zealand prime minister also apologized to Dotcom for the surveilling of his home, as surveillance of legal residents is forbidden in New Zealand. Graeber, *supra* note 1, at 200. Living abroad, Dotcom has even relaunched a new file-storage service in January 2013 called Mega. See David Kravets, *File-Sharing Service Mega Is No Megaupload*, WIRED (Jan. 22, 2013, 3:24 PM), <http://www.wired.com/threatlevel/2013/01/mega-is-no-megaupload/> (“All Mega appears to be is a storage service that allows the encrypted storage and transfer of files to other members.”).

<sup>198</sup> *United States v. Dotcom*, No. 1:12-cr-3, 2012 WL 4788433, at \*2 n.6 (E.D. Va. Oct. 5, 2012) (order denying motion to dismiss the indictment). The district court refused to dismiss the case because, it reasoned, the government may be able to comply with the rule by serving process on one of the operators of Megaupload, once extradited, and that service may be construed as service on the company if the court can pierce the corporate veil. *Id.* at \*1–\*2.

<sup>199</sup> *Cf.* 18 U.S.C. § 3184 (2012) (criminal extradition statute). Generally under this statute, the defendant must have been charged “with having committed within the jurisdiction of any such foreign government any of the crimes provided for by [an extradition] treaty or convention” and then must be brought before a judge “to the end that the evidence of criminality may be heard and considered.” *Id.*

<sup>200</sup> See *Graduate Mgmt. Admission Council v. Raju*, 241 F. Supp. 2d 589, 597–600 (E.D. Va. 2003). In *Raju*, a citizen of India was using a foreign website to sell copyrighted study materials for the Graduate Management Admission Test primarily to U.S. students. *Id.* at 590–91. The district court held “that Raju’s contacts with the United States are sufficient to permit the exercise of personal jurisdiction” under Federal Rule of Civil Procedure 4(k)(2) because he “directed his activities at the United States market” and yet “did not sufficiently direct his activities at any given state to justify a finding of personal jurisdiction in any state court.” *Id.* at 600. The court added that:

To find otherwise would not only frustrate GMAC’s attempts in this case to vindicate its rights under United States law, by requiring GMAC to turn to foreign courts to vindicate those rights against a likely elusive defendant, it would also provide a blueprint whereby other individuals bent on violating United States trademark and copyright laws could do so without risking suit in a United States court.

*Id.*

a defendant's assets never touch U.S. soil, any judgment entered will likely never be enforced.<sup>201</sup>

Second, the federal government has the authority to quickly shutter infringing sites. Federal courts generally treat domain names as intangible property<sup>202</sup> located wherever the domain-name registry or registrar is.<sup>203</sup> Because of this understanding, the U.S. government has grounds for *in rem* jurisdiction over millions of domain names, as the registry for all .com and .net domain names is controlled by a Virginia company.<sup>204</sup> This jurisdictional hook allows the government to shut down even foreign sites by seizing them through civil forfeiture,<sup>205</sup> as it did with "Operation in Our

---

<sup>201</sup> *Raju* resulted in a default judgment. *Id.* at 600.

<sup>202</sup> See, e.g., *CRS Recovery, Inc. v. Laxton*, 600 F.3d 1138, 1142 (9th Cir. 2010) ("Like the majority of states to have addressed the issue, California law recognizes a property interest in domain names.") The *Laxton* court also quotes that "'courts generally hold that domain names are subject to the same laws as other types of intangible property.'" *Id.* (quoting JONATHAN D. HART, *INTERNET LAW* 120 (6th ed. 2008)).

<sup>203</sup> The Ninth Circuit in *Office Depot Inc. v. Zuccarini*, 596 F.3d 696, 702 (9th Cir. 2010), for example, decided that, under California law, domain names were located where the registry was located for the purpose of asserting *quasi in rem* jurisdiction.

<sup>204</sup> See Belleville, *supra* note 8, at 315 ("Any web sites with a '.com' or '.net' top level domain name are hosted at a registry operated by Verisign, Inc. in Virginia."); David Kravets, *Uncle Sam: If It Ends in .Com, It's Seizable*, WIRED (Mar. 6, 2012), <http://www.wired.com/threatlevel/2012/03/feds-seize-foreign-sites/> ("A complicated web of bureaucracy and Commerce Department-dictated contracts signed in 1999 established that key domains would be contracted out to Network Solutions, which was acquired by VeriSign in 2000. That cemented control of all-important .com and .net domains with a U.S. company—VeriSign—putting every website using one of those addresses firmly within reach of American courts regardless of where the owners are located—possibly forever.").

<sup>205</sup> See 18 U.S.C. §§ 981, 2323 (2012); see also *United States v. Davis*, 628 F.3d 84, 96 (2d Cir. 2011) (explaining that, when civil forfeiture is used in actions not brought under a civil forfeiture statute, as when "Immigration and Customs Enforcement officers acting pursuant to their authority under 19 U.S.C. §§ 1595 and 1595a," the government must establish probable cause that the property is being used for unlawful activity); see also 18 U.S.C. § 983(c)(1) (explaining that, otherwise, the burden of proof is preponderance of the evidence).

Sites.”<sup>206</sup>

Third, in a criminal proceeding, the government is able to freeze or seize all sorts of assets it believes are instruments or proceeds of criminal activity.<sup>207</sup> Megaupload’s assets subject to forfeiture included a slew of domain names, computer servers, bank accounts, vehicles, and expensive electronics.<sup>208</sup> Although a New Zealand court eventually returned some of these assets as improperly seized under New Zealand law,<sup>209</sup> assets in Hong Kong and the United States were also frozen or seized, including servers in Virginia.<sup>210</sup> An unfortunate side effect of these actions is that

---

<sup>206</sup> See Jack Mellyn, “*Reach Out and Touch Someone*”: The Growing Use of Domain Name Seizure as a Vehicle for the Extraterritorial Enforcement of U.S. Law, 42 GEO. J. INT’L L. 1241, 1254 (2011) (explaining how, during Operation in Our Sites, “seizure warrants were obtained from a federal judge and were served on Verisign, the Virginia-based administrator responsible for maintaining the authoritative list of .com and .net domain names”). This procedure was not necessary with Megaupload, however, as the company used a Washington-based domain-name registrar and located 525 of its computer servers in Virginia, where the indictment was filed. Indictment, *supra* note 80, at 19; *see also* Kravets, *supra* note 204 (“[T]he issue of the U.S.’s legal dominion claim over all .com domains wasn’t an issue in the January seizure of the domain of megaupload.com, which is implicated in one of the largest criminal copyright cases in U.S. history. Megaupload.com was registered in the United States with a registrar based in Washington state.”); Nate Anderson, *Explainer: How Can the US Seize a “Hong Kong site” like Megaupload?*, ARS TECHNICA, (Jan. 20, 2012, 5:05 PM), <http://arstechnica.com/tech-policy/2012/01/explainer-how-can-the-us-seize-a-hong-kong-site-like-megaupload/>.

<sup>207</sup> FED. R. CRIM. P. 32; *see also* 18 U.S.C. § 2323; Lee, *supra* note 75, at 65–67 (discussing the government’s seizure of Megaupload assets). The government must comply with the Fourth Amendment, of course, but courts are still working out the extent of these protections in the digital age. A fuller analysis of the Fourth Amendment’s application to seizures of computer data is outside the scope of this Article. The Authors recommend Professor Orin Kerr’s comprehensive article on the topic as a good starting point. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 547–65 (2005).

<sup>208</sup> Indictment, *supra* note 80, at 83–89. The vehicles included two Mercedes-Benz ML63 AMG with vanity plates reading “MAFIA” and “GUILTY.” *Id.* at 87.

<sup>209</sup> *See supra* note 197.

<sup>210</sup> Timothy Lee, *Feds: We Can Freeze Megaupload Assets Even if Case Dismissed*, WIRED (July 27, 2012, 5:30 PM), <http://www.wired.com/threatlevel/>



some of Megaupload's users lost access to lawfully stored data.<sup>211</sup>

Fourth, the government has a unique ability to collect evidence by search warrant, rather than subpoena. The Fourth Amendment limitations of computer searches are, like the rules for data seizure, still being defined, as computers fit poorly into canons developed around searches of people's homes.<sup>212</sup> But in the Megaupload case, the government's search powers led to the collection of scores of incriminating internal communications from the Mega-conspirators.<sup>213</sup> Technology journalists speculate that the FBI planted spyware<sup>214</sup> to collect data from the Mega-conspirators'

---

2012/07/megaupload-freeze/; see also Chester Yung, *Hong Kong Freezes Megaupload Assets*, WALL ST. J. (Jan. 21, 2012, 5:50 AM), <http://online.wsj.com/article/SB10001424052970204301404577174362457114578.html>.

<sup>211</sup> See Rebuttal Memorandum in Support of Renewal of Specially Appearing Defendant Megaupload Limited's Request for Dismissal of the Superseding Indictment Without Prejudice at 1, *United States v. Dotcom*, No. 1:12-cr-00003-LO, ECF Doc. No. 162 (E.D. Va. Jan. 29, 2013). The Electronic Frontier Foundation filed briefs on behalf of Megaupload users affected by the seizure of the servers holding their data, arguing that the property should be returned under Federal Rule of Criminal Procedure 41(g) as obtained in "callous disregard" of their property rights. *Id.* at 1–2. Under Rule 41(g), any "person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return." Negotiations are still ongoing regarding the fate of this data, which is currently being stored, at great expense, by Carpathia Hosting, the company that leased the servers to Megaupload. See Timothy B. Lee, *ISP: Storing 25 Petabytes of Megaupload Data Costs Us \$9,000 a Day*, ARS TECHNICA (Mar. 22, 2012, 2:45 PM), <http://arstechnica.com/tech-policy/2012/03/isp-storing-25-petabytes-of-megaupload-data-costs-us-9000-a-day/>.

<sup>212</sup> Kerr, *supra* note 207, at 536–40; see also *United States v. Flores-Lopez*, 670 F.3d 803 (7th Cir. 2012) (addressing the application of the Fourth Amendment to a cell phone and noting that "a modern cell phone is a computer").

<sup>213</sup> See Greg Sandoval & Declan McCullagh, *Feds: We Obtained MegaUpload Conversations with Search Warrant*, CNET (Jan. 31, 2012, 4:19 AM), [http://news.cnet.com/8301-31001\\_3-57368523-261/feds-we-obtained-megaupload-conversations-with-search-warrant/](http://news.cnet.com/8301-31001_3-57368523-261/feds-we-obtained-megaupload-conversations-with-search-warrant/).

<sup>214</sup> Merriam-Webster's online dictionary defines "spyware" as "software that is installed in a computer without the user's knowledge and transmits information about the user's computer activities over the Internet." Spyware Definition, MERRIAM-WEBSTER.COM, <http://www.merriam-webster.com/dictionary/spyware> (last visited Sept. 1, 2013).

local hard drives, because the government has produced five-year-old instant messages the conspirators sent via Skype, an online video-chatting service, which only stores messages for thirty days.<sup>215</sup> Suffice it to say, these records are unlikely to have been discovered through civil litigation.<sup>216</sup>

Fifth, there are potential benefits to pursuing criminal restitution rather than civil damages. To be sure, in a typical criminal copyright case, criminal restitution may limit an injured party's recovery. The Mandatory Victim Recovery Act<sup>217</sup> authorizes compensation only for victims' actual losses; recovery of an infringer's profits is saved for civil means.<sup>218</sup> Moreover, actual losses can be especially hard to prove in copyright-infringement cases because the number of people who download free or reduced-price infringing products may not accurately reflect the size of those products' legitimate customer base.<sup>219</sup> Nonetheless,

---

<sup>215</sup> Sandoval & McCullagh, *supra* note 213. Only emails, not Skype chats, are listed in the indictment of Megaupload; the Skype chats were disclosed by the FBI during proceedings in New Zealand related to its investigation of the company. *Id.*

<sup>216</sup> For another tale of the government using its powers to gather evidence against an alleged secondary copyright infringer, Brian McCarthy of Channelsurfing.net, see Nate Anderson, *Illegal TV Streamers, Here's How the Feds Will Hunt You Down*, ARTS TECHNICA (Mar. 3, 2011, 7:52 PM), <http://arstechnica.com/tech-policy/2011/03/illegal-tv-streamers-heres-how-the-feds-will-hunt-you-down/>.

<sup>217</sup> 18 U.S.C. § 3663(a)(1) (2012).

<sup>218</sup> See, e.g., *United States v. Fair*, 699 F.3d 508, 513–16 (D.C. Cir. 2012). The D.C. Circuit, in *Fair*, referred to decisions from the Second, Third, Fourth, Fifth, Seventh, Eighth, Ninth, and Tenth Circuits in declaring that “[t]he circuit courts of appeals are in general agreement that the defendant’s gain is not an appropriate measure of the victim’s actual loss in MVRA calculations.” *Id.* The D.C. Circuit then reversed a restitution award against an infringer who had sold illicit copies of Adobe software because the government had only proven the defendant’s profits, not Adobe’s actual loss. *Id.* at 514–16. The court noted that crime victims “may” achieve disgorgement of profits and ill-gotten gains through other statutory and civil-recovery mechanisms.” *Id.* at 514.

<sup>219</sup> *Id.* at 515 (noting that there was no evidence that an infringer’s customers would have purchased full-price products from the copyright holder); see also *United States v. Hudson*, 483 F.3d 707, 710 (10th Cir. 2007) (expressing skepticism that customers agreement to purchase reduced-price software proves

there is at least one potential benefit of restitution: restitution allows one court to divvy up relief to all injured parties in a proceeding spearheaded by the government, whereas litigation may proceed piecemeal led by the few rights-holders with the means to advance their cause.<sup>220</sup> Thus, restitution may be preferable when the potential victims are numerous, as is the case with file-sharing services.

Given the benefits of criminal prosecution, it is perhaps curious that the government has not gone after other delinquent file-sharing services. Florida-based Grooveshark, for example, has been sued by major music labels EMI and Universal for more than \$15 billion in damages,<sup>221</sup> and five other sites—including China's Baidu and Germany's RapidShare—were listed along with The Pirate Bay by Congress's International Anti-Piracy Caucus as "overwhelmingly used for the global exchange of illegal movies, music and other copyrighted works."<sup>222</sup> There are jurisdictional problems, however, with targeting foreign sites and inherent inefficiencies in prosecuting Grooveshark when civil litigation against it is ongoing. Mostly, though, the existence of these other sites again illustrates the importance of prosecutorial discretion: prosecutorial powers should be used only after authorities collect the type of evidence of profiteering and defiance of civil copyright laws exhibited by services like Megaupload and The Pirate Bay.

---

that they "would have agreed to purchase the same number of copies from [the copyright holder] Microsoft").

<sup>220</sup> A federal court must order restitution to any victim of copyright infringement under 18 U.S.C. § 2323(c) and in accordance with 18 U.S.C. §§ 3556, 3663A, and 3664. See 5 NIMMER & NIMMER, *supra* note 35, at § 15.07 [C][2].

<sup>221</sup> See Steve Musil, *Grooveshark Now Feels Lawsuit Wrath of All Major Music Labels*, CNET, (Jan. 5, 2012, 8:51 PM), [http://news.cnet.com/8301-1023\\_3-57353515-93/grooveshark-now-feels-lawsuit-wrath-of-all-major-music-labels/](http://news.cnet.com/8301-1023_3-57353515-93/grooveshark-now-feels-lawsuit-wrath-of-all-major-music-labels/); Graeme McMillan, *Universal Music Sues Music Streaming Service for 100,000 Illegal Uploads*, TIME (Nov. 21, 2011), <http://www.digitalmusicnews.com/permalink/2011/111123grooveshark>.

<sup>222</sup> Hatch, *International Anti-Piracy Caucus Unveils "2010 International Piracy Watch List"*, *supra* note 195.

## VI. CONCLUSION

This Article thus concludes with a note of caution. Given the history of increasingly severe criminal penalties for copyright infringement under U.S. law, there is every reason to expect that federal prosecutors will continue to wield a “big stick” against file-sharing services. As this Article has emphasized, there are advantages and efficiencies to criminal prosecutions over civil lawsuits: the federal government wields power to seize sites, to extradite, to freeze assets, and to record internal conversations surreptitiously as means to deter those file-sharing services refusing to comply with civil-enforcement efforts. And because prosecutorial discretion is more efficient than ill-advised attempts at blanket enforcement, this Article provides guidelines for the exercise of that discretion. Specifically, prosecutors should look for situations where liability under civil law is clearly established and civil enforcement is likely to be futile, and they should aim to prosecute the most prominent infringing services fitting those criteria.

But a prosecutor’s circumspection accomplishes more than just efficiency. Megaupload has not been convicted, and may never be, yet its business has been shut down, its assets frozen, its customers left unable to retrieve even lawfully stored data. Some of this smacks of the treatment of the King’s Messenger: punishment first, with trial after.<sup>223</sup> As argued, when the alleged conduct is egregious, and civil lawsuits are ineffective, then a criminal prosecution, with all its attendant hardships for the accused, may be warranted. But the guidelines here are intended as limitations, not as a call to pursue more prosecutions. Because the powers of federal prosecutors are great, a reluctance to use those powers is a virtue that preserves liberty.

---

<sup>223</sup> In *Through the Looking-Glass*, the White Queen tells Alice (the titular heroine of *Alice’s Adventures in Wonderland*) about the temporal predicament of the King’s Messenger, who is “in prison now, being punished: and the trial doesn’t even begin till next Wednesday: and of course the crime comes last of all.” See LEWIS CARROLL, *THROUGH THE LOOKING-GLASS AND WHAT ALICE FOUND THERE* 77–78 (Florence Milner ed., Rand McNally & Co. 1917). Alice is horrified. *Id.* “Suppose he never commits the crime?” she asks. *Id.* But the White Queen points out that he would be the better for it; after all, when someone commits a crime and is punished, they are the better for it—so it must be better still if they can be punished without having committed the crime at all. *Id.*



# **NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY**

**VOLUME 15, ISSUE 2  
JANUARY 2014**

Published by:



University of North Carolina School of Law  
Chapel Hill, North Carolina

## COPYRIGHT POLICY

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the *North Carolina Journal of Law & Technology* must be honored; copyright to each article is owned by its respective author(s). Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or a fee. To request permission, e-mail [info@ncjolt.org](mailto:info@ncjolt.org), contact the Editor-in-Chief at the below mailing address, or contact the author of the article.

Copyright © 2014, North Carolina Journal of Law & Technology.  
All rights reserved.

## SUBSCRIPTIONS AND BACK ISSUES

The *North Carolina Journal of Law & Technology* publishes four issues per volume: two in the Fall and two in the Spring. Annual subscriptions are \$40 for the complete volume. For more information or to subscribe, visit [ncjolt.org](http://ncjolt.org), e-mail [info@ncjolt.org](mailto:info@ncjolt.org), or contact the Managing Editor at the following address:

North Carolina Journal of Law & Technology  
University of North Carolina School of Law  
Van Hecke-Wettach Hall  
160 Ridge Road, CB #3380  
Chapel Hill, North Carolina 27599-3380

Articles are available online at [ncjolt.org](http://ncjolt.org) and through Lexis-Nexis, Westlaw, and Hein Online subscription services. Back issues and complete sets of the *North Carolina Journal of Law & Technology* may be ordered directly from William S. Hein & Co., 1285 Main Street, Buffalo, New York 14209-1987. Orders may also be placed by calling Hein at (800)-828-7571, via fax at (716)-883-8100, or e-mail to [order@wshein.com](mailto:order@wshein.com).

## PUBLICATION INFORMATION

The text and citations of the *North Carolina Journal of Law & Technology* conform to *The Bluebook: A Uniform System of Citation* (19th ed. 2010). Materials cited “on file with the *North Carolina Journal of Law & Technology*” will be retained for a maximum of five years from date of publication. The journal is printed by Joe Christensen, Inc. in Lincoln, Nebraska. Publication number ISSN: 1542-5177.

## SPONSORS

The *North Carolina Journal of Law & Technology* would like to thank the generous contributors who have helped make this journal possible:

### *Benefactors:*



The University of  
North Carolina at Chapel Hill  
Student Congress

Anne Klienfelter, Associate Professor of Law and Director of the  
Law Library, UNC School of Law

### *Patrons:*



UNC  
GRADUATE *and* PROFESSIONAL  
STUDENT FEDERATION

UNC  
CENTER FOR  
MEDIA LAW &  
POLICY

This publication is funded in part by Student Fees that were appropriated and disbursed by the Student Government at the University of North Carolina at Chapel Hill and the Student Bar Association of the University of North Carolina School of Law.



## BOARD OF ADVISORS

- CASSIE ANDERSON—Greenberg Traurig LLP; *N.C. JOLT* Editor-in-Chief, Vol. 12
- LISA ARTHUR—Smith Moore Leatherwood, LLP; *N.C. JOLT* Editor-in-Chief, Vol. 13
- ETHAN A. BERGHOFF—Baker & McKenzie LLP; *N.C. JOLT* Board Member
- ANDREW CHIN—Associate Professor of Law, UNC School of Law
- CHRISTINE H. DUPRIEST—Womble Carlyle Sandridge & Rice, LLP; *N.C. JOLT* Editor-in-Chief, Vol. 9
- JASON EVANS—McGuireWoods LLP; *N.C. JOLT* Editor-in-Chief and Founder, Vol. 1 & 2
- ELIZABETH D. FERRILL—Finnegan, Henderson, Farabow, Garrett & Dunner, LLP; *N.C. JOLT* Publication Editor, Vol. 7
- LESLIE T. GRAB, PH.D.—Kilpatrick Townsend & Stockton, LLP; *N.C. JOLT* Online Edition Editor, Vol. 9
- AARON R. HARMON—Clinical Assistant Professor of Law, UNC School of Law; *N.C. JOLT* Editor-in-Chief, Vol. 8; *N.C. JOLT* Faculty Advisor
- JEFFREY HOFFMAN—Simply Grid; Original Board Member
- ANNE KLINEFELTER—Associate Professor of Law and Director of the Law Library, UNC School of Law; *N.C. JOLT* Faculty Advisor
- TOD M. LEAVEN—The Dungan Law Firm; *N.C. JOLT* Editor-in-Chief, Vol. 11
- CAROLINE MEEK-PRIETO—Adams and Reese LLP; *N.C. JOLT* Editor-in-Chief, Vol. 10
- MARY U. MUSACCHIA—First Flight Venture Center, Inc. & Whitmeyer Tuffin, PLLC, Original Board Member
- BENTLEY J. OLIVE—Olive Law Group, PLLC; *N.C. JOLT* Executive Editor, Vol. 2
- STEPHEN PETROSKI—Myers, Bigel, Sibley & Sajovec, P.A.; *N.C. JOLT* Board Member
- ANDREW SALEK-RAHAM—Groom Law Group; *N.C. JOLT* Editor-in-Chief, Vol. 14
- DENISE WALKER—United States Attorney, Eastern District of North Carolina; *N.C. JOLT* Editor-in-Chief, Vol. 6
- RANDY WHITMEYER—Whitmeyer Tuffin PLLC; *N.C. JOLT* Board Member
- ALAN E. WROBEL—Managing Attorney, SAS Institute Inc; Original Board Member

# VOLUME 15, 2013–2014

*EDITOR-IN-CHIEF*  
HOLLY BANNERMAN

*EXECUTIVE EDITORS*  
KAITLIN POWERS  
VIRGINIA WOOTEN

*MANAGING EDITOR*  
JUSTIN MANN

*WEB EDITOR*  
ASHLEY MCALARNEY

*PUBLICATION EDITORS*  
TERESA COOK  
SEIKO OKADA

*SYMPOSIUM EDITOR*  
MIKE FRONGELLO

*SENIOR ARTICLES EDITOR*  
CARLA GRAY

## *ARTICLES EDITORS*

JONATHAN AMBROSE  
NEIL BARNES  
TASNEEM DHARAMSI

LAUREN POWERS  
ANNE MARIE TOSCO

## *NOTES EDITORS*

AMANDA JONES  
ANURADHA MADAN  
DYLAN MATAWAY-NOVAK

CARA RICHARDS  
LAURA ARREDONDO-SANTISTEBAN  
KATHERINE STREET

## *SENIOR STAFF MEMBERS*

KELLY ANDERSON

JENNIFER POLERA

AGNIESZKA ZMUDA

## *STAFF MEMBERS*

WILLIAM BLACKTON  
KERRY BOEHM  
DANIEL CHOO  
AMANDA COLLEY  
BRITTANY CROOM  
KETA DESAI  
NATALIE DEYNEKA  
KYLE EVANS  
DAVID FITZGERALD  
RORY FLEMING

IKEE GARDNER  
MATTHEW HENRY  
STELLA KREILKAMP  
GABRIEL KUSSIN  
CHRISTIAN LANDRETH  
BRITTON LEWIS  
TONY LUCAS  
TIMOTHY MCKEEVER  
KELLY MORRIS  
RYAN NILAND

DANIEL PARISI  
CATHERINE PEREZ  
AMELIA SERRAT  
MATTHEW SPANGLER  
BENJAMIN SZANY  
NICHOLAS TURZA  
MATTHEW VIVA  
LLOGAN WALTERS  
CHRISTINA WHEATON  
SAMUEL WILLIAMS

