Pornography, Piracy, and Privacy: How Adult Entertainment Companies' Mass Copyright Infringement Litigation Threatens Sexual Privacy, and What Courts Should Do About It

Matthew E. Kelley

George Washington University Law School
J.D., May 2012

I. Introduction

The accusation comes in a carefully worded letter from your Internet provider, or a more pointed missive from a law firm. Your IP address has been identified, it says, as participating in copyright infringement. That's bad enough, until you see the name of the work you're accused of stealing: *Amateur College Men Down on the Farm*,[1] or maybe *Teen Anal Sluts*.[2] If you're lucky, it's something respectable like *The Hurt Locker*;[3] if you're unlucky, it's something unprintable. Pay us, say, $3,500, the lawyers' letters say, or else: "we will have you personally named in the suit, and proceed directly against you."[4]

If this kind of notice appears in your mailbox, you're not alone. It's happened to a 70-year-old widow in San Francisco[5] and a legally blind network security expert in Seattle;[6] a Florida grandmother[7] and an Iraq war veteran in North Carolina[8]—more than 200,000 people in all, by some estimates.[9] These letters are part of a recent deluge of copyright infringement lawsuits involving the online sharing of video content, most of them filed by adult entertainment companies or independent filmmakers.[10] These cases name dozens, hundreds, or thousands of anonymous defendants each, identified only by Internet Protocol (IP) addresses of networked devices, but few people are ever named and actual trials are unprecedented.[11] Instead, plaintiffs

[1] Liberty Media Holdings, LLC v. BitTorrent Swarm, --- F.R.D. ---, 2011 WL 5190048, at *1 (S.D. Fla. Nov. 1, 2011).
[2] Complaint at 2, 4 Twenty Media Inc. v. Swarm Sharing Hash Files 6D59B29B0E51E9B5B4C0F9192CE99ED5EC5457E8, No. 6:12-cv-00031 (W.D. La. Jan. 10, 2012).
[3] Voltage Pictures v. Vazquez, --- F. Supp. 2d ---, 2011 WL 5006942, at *1 (D.D.C. Oct. 20, 2011).
[4] *Attorney Paul Lesko and 1000% Return on Investment in 'Teen Anal Sluts'*, Fight Copyright Trolls (Apr. 30, 2012), http://fightcopyrighttrolls.com/2012/04/30/attorney-paul-lesko-and-1000-return-on-investment-in-teen-anal-sluts/ (embedding and quoting from letter from attorney for 4 Twenty Media offering settlement to person accused of infringing *Teen Anal Sluts*); *see also* Keegan Hamilton, *Porn, Piracy & BitTorrent*, SEATTLE WEEKLY (Aug. 10, 2011), http://www.seattleweekly.com/2011-08-10/news/porn-piracy-bittorrent/.
[5] James Temple, *Lawsuit Says Grandma Illegally Downloaded Porn*, S.F. CHRON. (July 15, 2011), http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/07/14/BUG51KA26R.DTL&tsp=1.
[6] Hamilton, *supra* note 4.
[7] Pat Beall, *Porn Litigation: Film Studios Threaten, and Settle With, Possibly Guiltless Internet Users*, PALM BEACH POST (July 4, 2011, 4:13 PM), http://www.palmbeachpost.com/news/porn-litigation-film-studios-threaten-and-settle-with-1580504.html.
[8] Hamilton, *supra* note 4.
[9] *See infra* notes 97-100 and accompanying text.
[10] *See infra* Part III.C.
[11] *See id.*

use the litigation to gather names of alleged infringers who are then bombarded with emails, letters and phone calls seeking settlements of several thousand dollars.[12]

This current wave of mass copyright litigation has spawned a problem with infringement of a different kind: infringement of Internet users' rights to informational and sexual privacy. By seeking to squeeze settlements out of defendants by the thousands, without regard to whether or not they actually infringed anything, adult entertainment and independent film companies are jeopardizing the very rights that make their industries possible in the first place.

Courts should respond to this problem by strengthening existing procedural protections. Plaintiffs seeking subpoenas to identify alleged infringers of sexually explicit material should be held to stricter standards of proof, including evidentiary showings of copyright ownership and infringement. Courts should require plaintiffs seeking the identities of Internet users to use simple tools to provide a reasonable basis to believe that the court has personal jurisdiction over the putative defendants. Finally, courts should insist that plaintiffs have properly joined defendants in mass cases and, if not, sever the dozens, hundreds or thousands of defendants in suits where plaintiffs are misusing the system.

II. A Brief History of Online Copyright Infringement Litigation

Although the unlawful posting and sharing of copyrighted content online had been occurring since the early days of the Internet, online infringement exploded in the late 1990s with the emergence of peer-to-peer (P2P) file-sharing technology and Napster, the "first and most notorious P2P system."[13] Peer-to-peer software allows users to transfer files among themselves, rather than merely uploading and downloading files via a centralized server.[14] Napster provided free file-sharing software and servers to facilitate the file transfers, and

[12] *See id.*
[13] In re Charter Commc'ns, Inc., 393 F.3d 771, 773 (8th Cir. 2005).
[14] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 545 U.S. 913, 919-20 (2005).

maintained an index of available files which allowed users to search for particular content – usually songs – and then choose to connect with another user who had the desired file available to download.[15] That index was a key reason for Napster's downfall. The Northern District of California and the Ninth Circuit held that Napster was liable for contributory and vicarious copyright infringement because, among other reasons, its maintenance of the index showed it knowingly encouraged and assisted its users' infringement,[16] and had the means to control it.[17]

Second-generation P2P services such as Grokster, StreamCast, and KaZaA hoped to avoid Napster's mistakes. Unlike Napster, these newer systems dispersed the indexing functions and allowed users to connect directly.[18] In Grokster's system, for example, some users' computers were designated as "supernodes" that maintained temporary indices of the files available on a group of computers on the network; if the requested file was not available in the supernode's network, the request was relayed to other supernodes until the requested file was found and the requesting and providing computers could be connected directly.[19]

In the end, this decentralization was not enough to save Grokster and StreamCast, however. Reversing the lower courts, the Supreme Court ruled in 2005 that the services could be held liable for vicarious and contributory infringement, citing evidence their executives knew the networks were being used for infringement and that they intended such infringing uses, as exemplified by positioning themselves as alternatives to Napster when the courts clipped Napster's wings.[20]

---

[15] A&M Records, Inc. v. Napster, Inc. (*Napster I*), 239 F.3d 1004, 1011-13 (9th Cir. 2001).
[16] *Id.* at 1020-22.
[17] *Id.* at 1022-24.
[18] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 545 U.S. 913, 921-22 (2005).
[19] *Id.* at 921.
[20] *Id.* at 923-27 (2005). The Court dryly observed, for example, that "Grokster's name is an apparent derivative of Napster." *Id.* at 925.

Meanwhile, copyright holders' initial losses in their suits against intermediaries such as Grokster prompted the record labels to open another front in their legal war against online infringement: lawsuits against individual file sharers.[21] The labels' trade group, the Recording Industry Association of America (RIAA), in 2003 began directly suing individuals it accused of swapping infringing music files.[22] The RIAA's movie industry cousin, the Motion Picture Association of America (MPAA), announced its own lawsuits against individuals a year later.[23]

A. Failure of § 512(h) Subpoenas

When the RIAA first started suing individual infringers, its lawyers assumed they had a cheap and easy way to discover defendants' identities: using the expedited, *ex parte* subpoena provision of the Digital Millennium Copyright Act.[24] Under 17 U.S.C. § 512(h), copyright owners may petition a district court clerk to issue a subpoena to an online service provider seeking identifying information about an alleged infringer.[25] The law allows the clerk to issue such subpoenas without review by a judge or magistrate, so long as the proposed subpoena meets certain requirements and the copyright owner submits a signed statement declaring it will use the subpoenaed information only to protect its rights.[26] Another advantage is that the subpoenas can be obtained for a $35 fee,[27] not the filing fee for an actual lawsuit, which is currently $350.[28]

Unfortunately for the RIAA, several ISPs balked. They argued that § 512(h) applied only to ISPs that *stored* allegedly infringing files, not service providers acting merely as *conduits* for

[21] *See, e.g.*, Annemarie Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, 89 OR. L. REV. 81, 81 (2010); Justin Hughes, *On the Logic of Suing One's Customers and the Dilemma of Infringement-Based Business Models*, 22 CARDOZO ARTS & ENT. L. J. 725, 728 (2005).
[22] *See, e.g.*, Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1232 (D.C. Cir. 2003).
[23] Hughes, *supra* note 21, at 730.
[24] *See, e.g.*, In re Charter Commc'ns, Inc., 393 F.3d 771, 774 (8th Cir. 2005); Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1232 (D.C. Cir. 2003).
[25] 17 U.S.C. § 512(h)(1) (2006).
[26] *Id.* at § 512(h)(4).
[27] Kristina Groennings, Note, *Costs and Benefits of the Recording Industry's Litigation Against Individuals*, 20 BERKELEY TECH. L.J. 571, 574 (2005).
[28] 28 U.S.C. § 1914(a) (2006).

the allegedly infringing file transfers.[29] The District of Columbia and Eighth Circuits agreed,[30] dealing a serious setback to the recording industry's efforts to target individuals.[31]

Both circuits held that the subpoena provision was inapplicable because it requires the subpoena application to include a copy of a valid takedown notice under another provision of § 512.[32] The provisions of § 512 governing providers of online caching, storage and linking services require that upon notice by a copyright holder, the service must delete or block access to allegedly infringing material.[33] These notice and takedown provisions do not apply to ISPs that merely transmit data, however.[34] The reason is simple: if the ISP is not storing any allegedly infringing files, there's nothing for it to take down – the files reside on the alleged infringers' own computers.[35] Without anything to take down, there can be no takedown notice, and without a takedown notice, there can be no subpoena.[36]

B. Meet John Doe: Suing Defendants By IP Address

Because § 512(h) subpoenas are unavailable, as the Eighth Circuit noted in *Charter*, copyright owners must file "John Doe" lawsuits against individual alleged infringers – suing anonymous defendants in order to obtain court-ordered disclosure of identifying information from their ISPs.[37] In those cases, copyright holders attempt to sue alleged infringers directly,

---

[29] *Charter*, 393 F.3d at 775; *Verizon*, 351 F.3d at 1231. Section 512 provides other safe harbors for other online services: caching, the short-term storage of data incidental to transmission, § 512(b); storing material at the direction of users, § 512(c); and providing searching or linking services, § 512(c). Providers of these three services must block or remove infringing content when notified by copyright holders under the law's "notice and takedown" provisions. 17 U.S.C. §§ 512(b)(2)(E); (c)(1)(C) & (c)(3); (d)(3) (2006).

[30] *Charter*, 393 F.3d at 777, *Verizon*, 351 F.3d at 1236.

[31] *See* Pac. Century Int'l, Ltd. v. Does 1-37, --- F. Supp. 2d ---, Nos. 12 C 1057, 12 C 1080, 12 C 1083, 12 C 1085, 12 C 1086, 12 C 1088, 2012 WL 1072312, at *2 n.6 (N.D. Ill. Mar. 30, 2012) (noting that after *Verizon*, § 512(h) "became inadequate for digital copyright owners attempting to identify users downloading copyrighted material on P2P networks.").

[32] 17 U.S.C. § 512 (c)(3)(A) (2006); *Charter*, 393 F.3d at 777, *Verizon*, 351 F.3d at 1235.

[33] 17 U.S.C. §§ 512(b)(2)(E); (c)(1)(C) & (c)(3); (d)(3) (2006).

[34] *Id.*; *see also supra* note 29.

[35] *Charter*, 393 F.3d at 777, *Verizon*, 351 F.3d at 1235-36.

[36] Both circuits declined to reach the ISPs' other arguments: that the subpoena procedure violated the case or controversy requirements of Article III and infringed the First Amendment rights to anonymous speech of the targeted Internet users. *Charter*, 393 F.3d at 777-78; *Verizon*, 351 F.3d at 1231.

[37] *Id.* at 775 n.3 (suggesting that "organizations such as the RIAA can file a John Doe suit, along with a motion for third-party discovery of the identity of the otherwise anonymous 'John Doe' defendant.").

initially identifying only IP addresses associated with putative defendants.[38] Immediately after filing suit, the plaintiff files an *ex parte* motion for pre-service discovery, seeking approval to issue a traditional civil subpoena to an ISP for the identifying information about their subscribers associated with the offending IP addresses at the date and time specified.[39]

During the music industry's initial wave of John Doe lawsuits, courts usually granted the discovery motions and rejected arguments from the Doe defendants, ISPs and cyber liberties groups that the subpoenas should be quashed.[40] Once the record labels obtained the identifying information, they would notify the putative defendants and offer them the option of a quick, out-of-court settlement, to which most Does agreed.[41] The recording companies settled thousands of these lawsuits for thousands of dollars each.[42]

The RIAA gave up its litigation campaign against individual file sharers at the end of 2008, choosing instead to collaborate with other copyright owners and ISPs in an agreement to provide a "graduated response" to alleged infringement.[43] As the name suggests, graduated response means a series of escalating measures to deter and punish individual infringers. The sanctions begin with the ISP sending the user notifications of alleged violations and escalate to

---

[38] *See, e.g.*, Patrick Fogarty, *Major Record Labels and the RIAA: Dinosaurs in a Digital Age?*, 9 HOUS. BUS. & TAX L. J. 140, 156-57 (2008); Ashley I. Kissinger & Katharine Larsen, *Protections for Anonymous Online Speech*, 1068 PLI/PAT 815, 824 (2011) (hereinafter Kissinger & Larsen, *Protections*); Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1839-40 (2011).

[39] *See, e.g.*, Digital Sin, Inc. v. Does 1-176, No. 12-CV-00126 (AJN), 2012 WL 263491, at *1 (S.D.N.Y. Jan. 30, 2012) (describing plaintiff's *ex parte* motion for expedited discovery of putative defendants' identifying information and noting the proliferation of such actions across the country); Sony Music Ent'mt Inc. v. Does 1-40, 326 F.Supp.2d 556, 558-59 (S.D.N.Y. 2004) (discussing plaintiffs' motion for discovery); Joshua M. Dickman, *Anonymity and the Demands of Civil Procedure in Music Downloading Lawsuits*, 82 TUL. L. REV. 1049, 1059 (2008).

[40] *See, e.g., id.* ("Courts generally grant such expedited discovery as a matter of course."); Ashley I. Kissinger & Katharine Larsen, *Untangling the Legal Labyrinth: Protections for Anonymous Online Speech*, 13 J. INTERNET L. 1, 20 & n.30 (2010) (hereinafter Kissinger & Larsen, *Legal Labyrinth*).

[41] Dickman, *supra* note 39, at 1059-60 (noting that "after obtaining the Does' identities, the record companies almost always settle with each Doe."); Nick Mamatas, *Meet John Doe: The RIAA Runs Its Lawsuits as a Volume Business, and Sometimes Downloaders Just Gotta Settle*, VILLAGE VOICE, Mar. 7, 2005, http://www.villagevoice.com/music/0510,mamatas,61813,22.html (describing author's settling one such complaint and reporting the RIAA had settled 1,400 suits at that time).

[42] *Id.* (estimating an average settlement amount of $3,000). *See also, e.g.*, Hughes, *supra* note 21, at 749 (noting that estimates of the typical or average settlement ranging from $2,500 to $11,000.

[43] Bridy, *supra* note 21, at 81-84; John Eric Seay, Note, *Hang 'Em High: Will the Recording Industry Association of America's New Plan to Posse Up With Internet Service Providers In the Fight Against Online Music Piracy Finally Tame the Wild Internet?*, 16 J. INTELL. PROP. L. 269, 270 (2009).

restrictions such as "throttling down" the offending users' transmission speeds and, possibly (though this is not required), the online version of the death penalty: an ISP's termination of the user's Internet connection.[44] The entity created to oversee the process, the Center for Copyright Information, announced it would begin operations in the summer of 2012.[45]

III. BitTorrent: The New King of P2P File Sharing

After the demise of relatively centralized file-sharing facilitators such as Napster and Grokster, users increasingly shifted to BitTorrent technology.[46] Unlike Napster or Grokster, which were services that connected file sharers to each other, BitTorrent is software—at its most basic level, a protocol used to transfer data, like HTTP (HyperText Transfer Protocol), the file transfer technology used for webpages.[47] According to BitTorrent, Inc., as of December 2011 some 152 million computers worldwide had BitTorrent or the related µTorrent installed.[48]

A. The Swarm Downloading Innovation

Unlike other P2P systems in which one individual downloads a file directly from another individual, BitTorrent uses a "swarm" model to transfer files among users.[49] To prepare for sharing, a large file is sliced into pieces, each with a unique "hash "—a "digital fingerprint" identifying what part of what file it is.[50] The initial file sharer, or "seed," creates a "dot-torrent" file that consists of an index of the hash codes of the pieces of the desired work and a link to the

---

[44] Ctr. for Copyright Info., Copyright Alert System, http://www.copyrightinformation.org/alerts.
[45] Greg Sandoval, *Hollywood Formally Brings ISPs Into the Anti-Piracy Fight*, CNET NEWS (Apr. 2, 2012, 11:40 AM), http://news.cnet.com/8301-31001_3-57408208-261/hollywood-formally-brings-isps-into-the-anti-piracy-fight/?tag=mncol;txt.
[46] Jon Healy, *File Sharing: To Fight or Accommodate?*, L.A. TIMES (April 1, 2008), http://www.latimes.com/news/opinion/la-oew-healey1apr01,0,2014471.story ("The file-sharing protocol of choice these days is BitTorrent.").
[47] BitTorrent.com, A Beginner's Guide to BitTorrent, http://www.bittorrent.com/help/guides/beginners-guide.
[48] Press Release, BitTorrent, BitTorrent and µTorrent Software Surpass 150 Million User Milestone; Announce New Consumer Electronics Partnerships (Jan. 9, 2012), *available at* http://www.bittorrent.com/company/about/ ces_2012_150m_users. The company also claimed its technology accounts for 20% to 40% of global Internet traffic. *Id.*
[49] BitTorrent.com, User Manual: The Basics of BitTorrent, http://www.bittorrent.com/help/manual/chapter0201. *See also* Columbia Pictures Indus., Inc. v. Fung, No.CV 06-5778 (SVW)(JCx), 2009 WL 6355911, at *2-3 (C.D. Cal. Dec. 21, 2009).
[50] Bram Cohen, *Incentives Build Robustness in BitTorrent*, BITTORRENT.ORG, 2 (2003), http://www.bittorrent.org/bittorrentecon.pdf; BitTorrent.com, User Manual: Glossary, http://www.bittorrent.com/help/manual/glossary#hash.

"tracker," a server connected to the Internet that coordinates the sharing process for that file.[51] The seed then makes the dot-torrent file available to others, usually by posting it on a website.[52] Those wishing to download copies of the work click on the dot-torrent file to load it into their BitTorrent software, and the downloading process begins.[53]

BitTorrent makes its file transfers faster while using less Internet bandwidth by distributing the data transfer among its users.[54] During the file transfer process, the BitTorrent software takes pieces of the original file from all other "seeds" who are online and have the file available to download, as well as anyone else downloading the same file.[55] Instead of user A taking the entire copy of the file from user B, A gets bits of it from users B, C, D, E, and so on—and if user Z is downloading the same file, she may get bits of it from user A.[56] This feature of BitTorrent simultaneously decentralizes and speeds up the file sharing process while using less Internet bandwidth,[57] which makes the software particularly helpful for sharing large files such as movies.[58] Once the download is complete, the user can choose to remain connected and become a "seed" for future downloads of the same file.[59]

To use a rather oversimplified analogy, think of a data file as a book. To copy a whole book from just one other person, you'd have to copy each page from that one original—a fairly slow process, even with a speedy photocopier or scanner. BitTorrent is bit like assembling a copy of the book from a book group, each of whom has a copy of the book and can copy different chapters at the same time, vastly streamlining the copying process. Not only that, but to

---

[51] *Id.*
[52] Lei Guo et al., *A Performance Study of BitTorrent-Like Peer-to-Peer Systems*, 25 IEEE J. SELECTED AREAS IN COMMS. 155, 156 (2007), *available at* http://www.cse.ohio-state.edu/~etan/paper/JSAC2007.pdf.
[53] BitTorrent.com, A Beginner's Guide to BitTorrent, http://www.bittorrent.com/help/guides/beginners-guide.
[54] Cohen, *supra* note 50, at 1.
[55] Columbia Pictures Indus., Inc. v. Fung, No.CV 06-5778 (SVW)(JCx), 2009 WL 6355911, at *2 (C.D. Cal. Dec. 21, 2009); Guo, *supra* note 52, at 156.
[56] *Id.*
[57] Cohen, *supra* note 50, at 1.
[58] Healy, *supra* note 46.
[59] BitTorrent.com, A Beginner's Guide to BitTorrent, http://www.bittorrent.com/help/guides/beginners-guide.

take the analogy a bit further, when you're assembling the copied pages of the book from the book club, others who want the book can copy pages not only from members of the book group but also from those you already have received.

Although the BitTorrent file sharing process is more widely dispersed among different users, people wanting to find specific content and those wishing to offer that content, lawfully or otherwise, still have to be able to find each other. But there's no one central index or group of indices like the former Napster service had; instead, there are scores of websites that provide places to post and download dot-torrent files, indexed links to other websites hosting dot-torrent files, or both.[60] As with the Internet in general, there are sites that offer a wide range of material across genres and media types, and there are more specialized sites serving niche interests of their consumers. Although the most well-known and notorious torrent site is The Pirate Bay, which unabashedly offers access to thousands of infringing files,[61] there are sites offering music audio and video,[62] sites offering computer software,[63] sites offering public domain videos,[64] and, this being the Internet, a host of sites offering many different iterations of pornography.[65]

B. BitTorrent Technology and Copyright Law

BitTorrent has several significant features in the context of copyright infringement litigation. Unlike Napster, there's no single, centralized hub where users access an index of files and connect with each other; instead, there are thousands of individual torrent sites.[66] Further, neither the dot-torrent file nor the tracker computer includes any of the content of the file to be

[60] *See, e.g.*, Ernesto, *Top 10 Most Popular Torrent Sites of 2012*, TORRENTFREAK (Jan. 7, 2012), http://torrentfreak.com/top-10-most-popular-torrent-sites-of-2012-120107/.
[61] *Id.*
[62] *See, e.g.*, Jamendo, http://www.jamendo.com/en (last visited April 8, 2012).
[63] *See, e.g.*, Linuxtracker, http://linuxtracker.org (last visited April 8, 2012).
[64] *See, e.g.*, Public Domain Torrents, http://www.publicdomaintorrents.net (last visited April 8, 2012).
[65] *See, e.g.*, Enigmax, *Cheggit, Longstanding Adult BitTorrent Site, Calls it Quits*, TORRENTFREAK (Jan. 30, 2012), http://torrentfreak.com/cheggit-long-standing-adult-bittorrent-site-calls-it-quits-120130/ (discussing decisions by several torrent sites specializing in pornography to shut down because of pressure from copyright owners).
[66] *See, e.g.*, Paul Gil, *Best Torrents: The Top 35 Torrent Download Sites of 2012*, ABOUT.COM INTERNET FOR BEGINNERS (Apr. 12, 2012), http://netforbeginners.about.com/od/peersharing/a/torrent_search.htm.

shared.[67] Some operators of torrent sites have pointed to this fact to argue that the dot-torrent file and tracker are neither themselves infringing nor subject to notice and takedown under § 512.[68] The Pirate Bay, for example, made this argument in a profanity-laced response to a takedown notice from DreamWorks involving the movie *Shrek 2*.[69]

However, a California federal court hearing a secondary infringement lawsuit against the operator of several torrent sites held that downloading a dot-torrent file constitutes direct infringement, because doing so automatically connects the user to the swarm to start sharing the infringing file; thus, "it is clear that dot-torrent files and content files are, for all practical purposes, synonymous."[70] That case, *Columbia Pictures Industries v. Fung*,[71] illustrates how copyright holders' litigation against BitTorrent intermediaries has fared little better than in the initial stages of the litigation against Grokster. The lawsuit represents the movie industry's attempt to shut down Gary Fung, one of the largest operators of torrent search and indexing sites, including IsoHunt.com.[72] The trial court in 2009 granted plaintiffs' motion for summary judgment on liability, holding that Fung's sites were liable for inducement and contributory and vicarious infringement.[73] Fung appealed, and IsoHunt has remained online throughout more than

[67] *See* Cohen, *supra* note 50, at 2; Richard Raysman & Peter Brown, *Analyzing Novel Issues in Internet Jurisdiction*, N.Y.L.J. (Mar. 8, 2012), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1331083321177.
[68] *See* Ann Harrison, *The Pirate Bay: Here to Stay?*, WIRED (Mar. 13, 2006), http://www.wired.com/science/discoveries/news/2006/03/70358?currentPage=all.
[69] Clive Thompson, *The BitTorrent Effect*, WIRED (Jan. 2005), http://www.wired.com/wired/archive/13.01/bittorrent.html (quoting the site's response, which read in part: "It is the opinion of ourselves and our lawyers that you are [expletive] morons.").
[70] Columbia Pictures Indus., Inc. v. Fung, No.CV 06-5778 (SVW)(JCx), 2009 WL 6355911, at *9 & n.18 (C.D. Cal. Dec. 21, 2009).
[71] Columbia Pictures Indus., Inc. v. Fung, No.CV 06-5778 (SVW)(JCx), 2009 WL 6355911 (C.D. Cal. Dec. 21, 2009).
[72] *Id.* at *1-2.
[73] *Id.* at *1.

six years of litigation,[74] albeit under a court order requiring the site to block access to certain torrent files identified through keyword filters programmed by the movie industry plaintiffs.[75]

The BitTorrent file sharing process is not only more distributed but more anonymous. Although downloaders can choose to see the IP addresses of others involved in the swarm, in general that information is invisible to the users.[76] Therefore, many BitTorrent users would not know even how *many* other users are "seeds" acting as sources for parts of the downloaded file, let alone the seeds' screen names or geographic locations.[77] The downloading swarms are coordinated not by any centralized service but by individual trackers, which automatically connect those who join the swarm to a random list of the available addresses from that swarm.[78] This is in contrast to Napster and Grokster, where each file was transmitted only from one user to another, either directly or through a central server, and the downloader usually chose from whom to download (and thus likely saw at least the screen name of that source).[79]

These features of BitTorrent also allow copyright holders to identify IP addresses of those involved in a particular swarm. To carry out its function of mediating the file transfers, the tracker computer records the IP addresses of swarm participants, as well as the date and time that each address connected to and disconnected from the swarm, and users can configure their BitTorrent software to read this information.[80] Thus, copyright holders or the investigation firms

---

[74] As of April 2012, the appeal of the case was pending at the Ninth Circuit. *See Legal Brief: Online Copyright Infringement*, Thompson Reuters News & Insight (Dec. 22,2011), http://newsandinsight.thomsonreuters.com/Legal/ News/2011/12_-_December/Lega_Brief_Online_copyright_infringement/.

[75] Mike Masnick, *Forced MPAA Filter on IsoHunt Means Legitimate Content Is Being Censored*, TECHDIRT (Apr. 9, 2012, 8:15 AM), http://www.techdirt.com/articles/20120406/17372118414/forced-mpaa-filter-isohunt-means-legitimate-content-is-being-censored.shtml (criticizing the court order).

[76] Pac. Century Int'l, Ltd. v. Does 1-37, --- F. Supp. 2d ---, Nos. 12 C 1057, 12 C 1080, 12 C 1083, 12 C 1085, 12 C 1086, 12 C 1088, 2012 WL 1072312, at *4 n.13 (N.D. Ill. Mar. 30, 2012) (noting that "a BitTorrent user need not communicate with other users in any other way" than the anonymous and automated file-sharing process).

[77] *Id.*

[78] Cohen, *supra* note 50, at 2; Guo, *supra* note 52, at 156.

[79] Declaration of Seth Schoen in Support of Reconsideration of December 21 Order at 2-3, Hard Drive Productions, Inc. v. Does 1-1,495, No. 1:11-cv-01741-JDB-JMF (D.D.C. Jan. 30, 2012).

[80] Cohen, *supra* note 50, at 2; Hamilton, *supra* note 4.

they hire[81] can tap into a swarm for a particular work and record all of the IP addresses involved.[82] The trackers' data is vulnerable to manipulation and errors, however, and without more sophisticated investigation can lead to a large number of false positives.[83] Sophisticated BitTorrent users know all of this, of course, and have developed methods intended to mask the IP addresses of computers participating in a swarm.[84]

Further complicating the legal landscape, BitTorrent users are increasingly shifting to technological variants that make the file sharing process even more decentralized and anonymous. One such development is the use of magnet links to replace dot-torrent files and trackers.[85] Instead of a dot-torrent file containing the URL of a tracker computer and the digital fingerprints of the pieces of a certain file, the magnet link is simply a snippet of data that, when read by the user's BitTorrent client software, allows that program to seek out and connect to the desired swarm.[86] When magnet links are used, the dot-torrent file still exists, but inside the swarm, not posted separately on a website.[87] The Pirate Bay, for example, stopped hosting trackers in 2009 and started using only magnet links in February 2012.[88]

---

[81] Many plaintiffs hire outside firms to find infringers. *See, e.g.*, Digital Sin, Inc. v. Does 1-176, No. 12-CV-00126 (AJN), 2012 WL 263491, at *1 (S.D.N.Y. Jan. 30 2012) ("Digital Sin contracted 'Copyright Enforcement Group' ('CEG'), a company that discovers copyright infringements and arranges for enforcement.").

[82] Kevin Bauer, et al., *Bitstalker: Accurately and Efficiently Monitoring BitTorrent Traffic*, 1 PROC. 2009 FIRST IEEE INT'L WORKSHOP INFO. FORENSICS & SECURITY 181, 181 (2009), *available at* http://cseweb.ucsd.edu/~dlmccoy/papers/bauer-wifs09.pdf; Michael Piatek, Tadayoshi Kono & Arvind Krishnamurthy, *Challenges & Directions for Monitoring P2P File Sharing Networks –or-Why My Printer Received a DMCA Takedown Notice*, TRACKING THE TRACKERS 1 (2008), http://dmca.cs.washington.edu/dmca_hotsec08.pdf. *See also* Hamilton, *supra* note 4.

[83] Bauer, *supra* note 82, at 181; Piatek, Kono & Krishnamurthy, *supra* note 82, at 2-5; *see also infra* note 114 and accompanying text.

[84] Ernesto, *Anonymous, Decentralized and Uncensored File Sharing is Booming*, TORRENTFREAK (Mar. 3, 2012), http://torrentfreak.com/anonymous-decentralized-and-uncensored-file-sharing-is-booming-120302/.

[85] Lucian Parfeni, *BitTorrent Magnet Links Explained*, SOFTPEDIA (Jan. 19, 2010, 3:54 PM), http://news.softpedia.com/news/BitTorrent-Magnet-Links-Explained-132536.shtml.

[86] *Id.*; Ernesto, *BitTorrent's Future? DHT, PEX and Magnet Links Explained*, TORRENTFREAK (Nov. 20, 2009), http://torrentfreak.com/bittorrents-future-dht-pex-and-magnet-links-explained-091120/.

[87] *Id.*

[88] Ernesto, *Torrent-less Pirate Bay Sees Massive Drop in Bandwidth*, TORRENTFREAK (Mar. 8, 2012), http://torrentfreak.com/torrent-less-pirate-bay-sees-massive-drop-in-bandwith-120308/ (noting that one reason the website switched to magnet links was that they contain much less data and thus use less Internet bandwidth).

C. A Torrent of Lawsuits

Beginning in 2010,[89] federal district courts have been hit with "a nationwide blizzard of civil actions brought by purveyors of pornographic films alleging copyright infringement by individuals utilizing a computer protocol known as BitTorrent."[90] Some larger, similar lawsuits were filed by those asserting ownership of copyrights in B-movies or independent films—most prominently for the Oscar-winning Iraq war drama *The Hurt Locker*, whose copyright owner filed suit in the U.S. District Court for the District of Columbia in 2010 and eventually listed 24,583 Doe defendants.[91] Most of the lawsuits alleging infringement by BitTorrent, however, have been filed by corporate entities alleging they hold copyrights to sexually explicit videos.[92]

As with the RIAA's Doe lawsuits, the latest swarm of BitTorrent copyright infringement complaints refer to the defendants by IP addresses, and the plaintiffs seek approval immediately after filing to issue subpoenas to ISPs in order to identify the subscribers associated with those IP addresses.[93] Sometimes all of the defendants are alleged to have participated in the same swarm

---

[89] *See* Rhett Pardon, *5 Porn P2P Suits in Past Week; Attorney Targets 44,000 Does*, XBIZ.COM (Sept. 12, 2011), http://www.xbiz.com/news/news_piece.php?id=138435&mi=all&q=BitTorrent (reporting that "porn consumer piracy claims first started appearing in federal courts" in the fall of 2010).

[90] *In re* BitTorrent Adult Film Copyright Infringement Cases, Nos. 11-3995 (DRH)(GRB), 12-1147 (JS)(GRB), 12-1150 (LDW(GRB), 12-1154 (ADS)(GRB), 2012 WL 1570765, at *2 (E.D.N.Y. May 1, 2012). *See also* Digital Sin, Inc. v. Does 1-176, No. 12-CV-00126 (AJN), 2012 WL 263491, at *1 (S.D.N.Y. Jan. 30 2012) (noting that "[l]itigation of this nature . . . is proliferating in this district and throughout the country."); David Kravets, *Biggest BitTorrent Downloading Case in U.S. History Targets 23,000 Defendants*, WIRED.COM THREAT LEVEL BLOG (May 9, 2011, 5:15 PM), http://www.wired.com/threatlevel/2011/05/biggest-bittorrent-case/.

[91] Voltage Pictures v. Vazquez, --- F. Supp. 2d ---, 2011 WL 5006942, at *1 (D.D.C. Oct. 20, 2011) (noting that plaintiff had filed an amended complaint in May 2011 "in which it listed 24,583 putative defendants and twelve named defendants"). *See also, e.g.*, Maverick Entm't Grp. v. Does 1-2,115, 276 F.R.D. 389, 391 (D.D.C. 2011) (plaintiff asserted it held copyrights in 13 motion pictures, including *Army of the Dead*, *Holy Hustler*, and *Stripper Academy*).

[92] *See, e.g.*, *Digital Sin*, 2012 WL 263491, at *1 (plaintiff alleged infringement of *My Little Panties #2*); First Time Videos, LLC v. Does 1-500, 276 F.R.D. 241, 244 (N.D. Ill. 2011) (plaintiff asserted ownership of copyright in adult videos). *See also* Christopher Swartout, Comment, *Toward a Regulatory Model of Internet Intermediary Liability: File-Sharing and Copyright Enforcement*, 31 NW. J. INT'L L. & BUS. 499, 511 (2011) ("In addition to independent film makers, pornography companies have also sought to use the tactics of mass suits"); Beall, *supra* note 7.

[93] *See, e.g.*, MCGIP, LLC v. Does 1-149, No. C 11-02331 LB, 2011 WL 4352110, at *4 n.5 (N.D. Cal. Sept. 16, 2011) (describing this process).

downloading the same work,[94] while in other cases plaintiffs seek to identify those alleged to have infringed one of several different works.[95]

The dramatic difference between the RIAA lawsuits and the current swarm of BitTorrent cases is the number of defendants named in each suit. During its litigation campaign against individual file sharers, the RIAA sued a total of more than 35,000 individuals.[96] BitTorrent lawsuit plaintiffs, by contrast, have named hundreds of thousands of John Doe defendants in a little more than two years, often in cases with hundreds or thousands of defendants each. The Electronic Frontier Foundation, for example, estimated in July 2011 that some 150,000 Doe defendants had been sued;[97] *U.S. News & World Report* estimated in February 2012 that the number of defendants had reached 220,000;[98] and the BitTorrent enthusiast blog TorrentFreak estimated the total at 250,000 in December 2011.[99] A simple federal docket search performed in February 2012 found at least 318 infringement cases involving video content shared via BitTorrent filed between Jan. 1, 2010 and Feb. 15, 2012, against188,515 Doe defendants.[100]

A small subset of those cases was responsible for the vast majority of defendants. Just 46 cases in the sample targeted 1,000 or more IP addresses each for a total of 155,438 Does, more than 82% of the overall universe of defendants found by this search. The three largest cases—against 24,583 defendants, 23,322 defendants, and 15,551 defendants each—accounted for more

---

[94] *See, e.g.*, Liberty Media Holdings, LLC v. BitTorrent Swarm, --- F.R.D. ---, 2011 WL 5190048, at *1 (S.D. Fla. Nov. 1, 2011).
[95] *See, e.g.*, *Maverick Entertainment*, 276 F.R.D. at 391 (plaintiff alleged infringement of 13 movies).
[96] Eliot Van Buskirk, *RIAA to Stop Suing Music Fans, Cut Them Off Instead*, WIRED (Dec. 19, 2008, 7:26 AM), http://blog.wired.com/business/2008/12/riaa-says-it-pl.html.
[97] Beall, *supra* note 7.
[98] Jason Koebler, *Porn Companies File Mass Piracy Lawsuits: Are You at Risk?*, U.S. NEWS & WORLD REP. (Feb. 2, 2012), http://www.usnews.com/news/articles/2012/02/02/porn-companies-file-mass-piracy-lawsuits-are-you-at-risk.
[99] Ernesto, *Hurt Locker BitTorrent Lawsuit Dies, But Not Without Controversy*, TORRENTFREAK (Dec. 22, 2011), http://torrentfreak.com/hurt-locker-bittorrent-lawsuit-dies-but-not-without-controversy-111222/.
[100] The author used the Bloomberg Law database to search federal dockets for copyright infringement cases in which "Does" were listed as defendants and the pleadings included the word "BitTorrent." This limited search necessarily missed an unknown number of cases in which the pleadings did not mention BitTorrent by name, did not refer to defendants as "Does," or were not catalogued as such in the Bloomberg database. Also added to this total were seven cases filed in West Virginia that engendered a news release from the Electronic Frontier Foundation when the judge severed all but one defendant in each case. *West Virginia Copyright Troll Lawsuits*, Electronic Frontier Foundation, https://www.eff.org/cases/west-virginia-copyright-troll-lawsuits (last visited Apr. 21, 2012).

than a third of all defendants.[101] Adult entertainment companies were the plaintiffs in the majority of these large cases: twenty-seven of 46 cases, accounting for 61,184 defendants.

Plaintiffs in this latest round of Doe lawsuits, like the RIAA, seek settlements rather than trials.[102] There is not a single reported case involving a trial of one of these suits, and even naming identified defendants is quite rare.[103] Pre-litigation settlement amounts reportedly range from $1,000 to $6,000.[104] Default judgments or post-litigation settlement agreements have been as high as $20,000.[105] One defendant who acknowledged distributing several pornographic videos using BitTorrent agreed to a settlement with a face value of $250,000, though the agreement states that he "has the opportunity to reduce the amount payable" by ceasing infringing activities and making payments pursuant to a schedule not filed with the court.[106]

IV. The Big Shakedown: Concerns Raised By the John Doe Lawsuits

The size and nature of these BitTorrent lawsuits have raised serious questions about plaintiffs' practices. Judges have sanctioned plaintiffs' attorneys[107] and decried their litigation and settlement tactics as potentially abusive[108] and otherwise improper.[109] Some of those

[101] Voltage Pictures v. Vazquez, --- F. Supp. 2d ---, 2011 WL 5006942, at *1 (D.D.C. Oct. 20, 2011) (amended complaint listed 24,583 Doe defendants); Nu Image Inc. v. Does 1-23,322, 799 F. Supp. 2d 34, 37 & n.1 (D.D.C. 2011) (noting that plaintiff's counsel had brought other suits including one with 15,551 Doe defendants).
[102] Swartout, *supra* note 92, at 506-07; Beall, *supra* note 7; Koebler, *supra* note 98.
[103] *See infra* note 112 and accompanying text.
[104] Beall, *supra* note 7.
[105] *See, e.g.*, Liberty Media Holdings, LLC v. Does 1-62, No. 11-CV-575-MMA-NLS, 2011 WL 6934460, at *2 (S.D. Cal. Dec. 30, 2011) (approving a $20,000 settlement agreement with one defendant); Liberty Media Holdings, LLC v. Does 1-62, No. 11-CV-575-MMA-NLS, 2011 WL 4715172, at *2 (S.D. Cal. Oct. 6, 2011) (same).
[106] Consent Judgment Against Dedendant Tyler Schwaller, Liberty Media Holdings, LLC v. Schwaller, No. 10-CV-2625-LAB-CAB (S.D. Cal. Feb. 4, 2011).
[107] *See* Patrick Collins, Inc. v. Does 1-25, No. 11-cv-60571, 2012 WL 27586, at *2-3 (S.D. Fla. Jan. 4, 2012) (dismissing case as sanction for plaintiff's counsel's "abusive litigation tactic" in signing unrepresented defendant's name to pleading); *see also infra* notes 124-127 and accompanying text.
[108] Third Degree Films, Inc. v. Does 1-131, No. 12-108-PHX-JAT, 2012 WL 692993, at *7 (D. Ariz. Mar. 1, 2012). (expressing agreement with other courts' concerns that plaintiffs' "invasive discovery could lead to abusive settlement practices"); Hard Drive Prods., Inc. v. Does 1-130, No. C-11-3826 DMR, 2011 WL 5573960, at *3 (N.D. Cal. Nov. 16, 2011) ("[T]he court shares the concern that these cases potentially open the door to abusive settlement tactics").
[109] *See, e.g.*, K-Beech, Inc. v. Does 1-41, No. V-11-46, 2012 WL 773683, at *5 & n.2 (S.D. Tex. Mar. 8, 2012); SBO Pictures, Inc. v. Does 1-3,036, No. 11-4220 SC, 2011 WL 6002620, at *4 (N.D. Cal. Nov. 30, 2011).

targeted as putative defendants, together with cyber liberties organizations such as the Electronic Frontier Foundation, have fought back with lawsuits and counterclaims against the plaintiffs.[110]

Courts and critics say the most basic problems with these suits are that the plaintiffs seem interested only in extracting settlements from the individuals identified by the subpoenaed ISPs, whether or not those subscribers actually engaged in infringing downloads, and the plaintiffs use the threat of court action and public humiliation to do so.[111] Court records and public statements by some of the plaintiffs' lawyers support this conclusion. For example, few plaintiffs ever name and serve any defendants; one plaintiffs' counsel, when ordered by a federal judge to provide statistics on how many defendants it had actually served, listed more than 100 cases it had filed against hundreds of defendants, and acknowledged it had not served a single defendant in any of them.[112] Another plaintiff's lawyer told a North Carolina federal court that, based on his knowledge of statistics from suits against thousands of people nationally, between 35% and 55% of "the Doe Defendants will settle very early in the litigation."[113]

The risk of false accusations of infringement is high. Computer science researchers have documented that not only do pirates insert innocent IP addresses into BitTorrent tracker logs, but also that 10 percent or more of the addresses listed in those tracker logs may be inaccurate.[114] Furthermore, an IP address often only identifies one ISP subscriber's wireless router, rather than

[110] *See, e.g.*, First Amended Complaint, Abrahams v. Hard Drive Prods., Inc., No. C 12-01006 JCS (N.D. Cal. Mar. 26, 2012); Answer and Counterclaims of Bailey Zwarycz, AKA John Does 116 and 117, Third Degree Films, Inc. v. Does 1-152, No. 1:11-cv-01833-BAH (D.D.C. Feb. 1, 2012); First Amended Complaint, Wong v. Hard Drive Prods., Inc, No. 5:12-CV-00469 (HRL) (N.D. Cal. Jan. 31, 2012).

[111] *See, e.g.*, Raw Films, Inc. v. Does 1-32, No. 1:11-CV-2939-TWT, 2011 WL 6840590, at *2 & n.5 (N.D. Ga. Dec. 29, 2011) ("The risk of inappropriate settlement leverage is enhanced in a case like this involving salacious and graphic sexual content where a defendant may be urged to resolve a matter at an inflated value to avoid disclosure of the content the defendant was accessing.").

[112] Exhibit A, Plaintiff's Response to Order to Show Cause, AF Holdings LLC v. Does 1-135, No. 11-CV-03336-LHK, at 4-6 (N.D. Cal. Feb. 24, 2012).

[113] Declaration in Opposition to Motion to Quash or Modify Subpoena, K-Beech, Inc. v. Does 1-39, No. 5:11-CV-00381-BO (E.D.N.C. Oct. 11, 2011).

[114] Bauer, *supra* note 82, at 181-86; Piatek, Kono & Krishnamurthy, *supra* note 82, at 2-5.

the actual device which allegedly downloaded the infringing file.[115] Thus, anyone in that subscriber's household – or anyone nearby using an unsecured connection or hacking into a password-protected connection – could be responsible for any activity at that address.[116] Therefore, as one court explained, identifying the subscriber to an IP address does *not* identify the person responsible for the alleged infringement: "the alleged infringer could be the subscriber, a member of his or her family, an employee, invitee, neighbor or interloper."[117]

Even some plaintiffs have acknowledged that their approach is certain to result in a number of false positives.[118] One plaintiff's lawyer admitted that roughly a *third* of the individuals identified by ISPs under the John Doe subpoenas are not the ones responsible for the allegedly infringing file sharing.[119] The judge in that case explained: "Counsel stated that the true offender is often the 'teenaged son ... or the boyfriend if it's a lady,'" or a neighbor or other third party who hijacked an unsecured or vulnerable wi-fi connection.[120] Opponents of these infringement suits have gone further, alleging that plaintiffs have deliberately avoided having torrent files and trackers taken down so they may use them as "honeypots" to lure unsuspecting individuals into downloading the files and thus becoming a defendant to an infringement lawsuit.[121]

Judges have concluded that some of the plaintiffs' lawyers have tried to dodge responsibility for improper tactics by dismissing defendants before they can complain to the court. A judge in the Eastern District of Virginia noted that some defendants complained that

---

[115] *In re* BitTorrent Adult Film Copyright Infringement Cases, Nos. 11-3995 (DRH)(GRB), 12-1147 (JS)(GRB), 12-1150 (LDW(GRB), 12-1154 (ADS)(GRB), 2012 WL 1570765, at *2 (E.D.N.Y. May 1, 2012).
[116] *Id.*
[117] *Id.* at 8. The court also noted that one of the plaintiffs claimed that it could hold the owner of an unsecured wireless connection responsible in negligence for infringing activity that took place over that connection, a contention the court said "flies in the face of common sense." *Id.* at 5-6 & n.3.
[118] Pac. Century Int'l Ltd. v. Does 1-101, No. C-110-02533 (DMR), 2011 WL 5117424, at *2 (N.D. Cal. Oct. 27, 2011).
[119] Digital Sin, Inc. v. Does 1-176, No. 12-CV-00126 (AJN), 2012 WL 263491, at *3 (S.D.N.Y. Jan. 30, 2012).
[120] *Id.*
[121] First Amended Complaint at ¶¶ 38-41, Wong v. Hard Drive Prods., Inc, No. 5:12-CV-00469 (HRL) (N.D. Cal. Jan. 31, 2012).

after plaintiffs obtained their information from ISPs, they started getting harassing phone calls demanding $2,900 settlements.[122] But when those defendants filed motions to dismiss or sever, the plaintiff immediately dismissed the case against them.[123]

A Texas judge uncovered more egregious misconduct by plaintiffs' attorney Evan Stone, who issued subpoenas to ISPs despite lacking any court authorization to do so.[124] Before ruling on whether the subpoenas should issue, the judge had appointed attorneys *ad litem* to represent the interests of the putative Doe defendants—but Stone dismissed the case before the *ad litem* lawyers could report back to the judge.[125] Stone nevertheless served subpoenas on ISPs, some of them on the same day he dismissed the case, as if they had been approved by the court.[126] Stone's misconduct earned him more than $32,000 in sanctions, a finding of contempt of court, and an order that he file a copy of the sanctions order in every federal and state proceeding in which he represented a party at the time of his misconduct.[127]

A series of Florida cases had even more fundamental problems—they were filed by a lawyer who was not licensed to practice in the state.[128] U.S. District Judge Robert Hinkle dismissed 27 lawsuits against 3,547 defendants in April 2012, pointing out that long before he filed the cases, Terik Hashmi had executed a cease-and-desist affidavit acknowledging he was not permitted to practice law in Florida and, except for participating in immigration cases, his doing so would constitute contempt of court and a third-degree felony.[129] More disturbingly, the

[122] Raw Films, Ltd. v. Does 1-32, No. 3:11cv532-(JAG), 2011 WL 6182025, at *2 (E.D. Va. Oct. 5, 2011).
[123] *Id.* The judge continued: "This course of conduct indicates that the plaintiffs have used the offices of the Court as an inexpensive means to gain the Doe defendants' personal information and coerce payment from them. The plaintiffs seemingly have no interest in actually litigating the cases, but rather simply have used the Court and its subpoena powers to obtain sufficient information to shake down the John Does." *Id.* at *3.
[124] Mick Haig Productions, e.K. v. Does 1-670, No. 3:10-CV-1900-N, 2012 WL 213701, at *1 (N.D. Tex. Jan. 24, 2012).
[125] *Id.*
[126] *Id.*
[127] *Mick Haig*, 2012 WL 213701, at *5.
[128] Rhett Pardon, *U.S. Judge Orders 27 Porn BitTorrent Piracy Suits Dismissed*, XBIZ.COM (Apr. 4, 2012, 1:45 PM), http://newswire.xbiz.com/view.php?id=146682.
[129] Order for Dismissal, Third Degree Films, Inc. v. Does 1-259, Consolidated Case No. 4:11cv570-RH/WCS (N.D. Fla. Apr. 2, 2012).

judge observed that Mr. Hashmi may have participated in extracting settlements from defendants who did not know he was not a licensed Florida attorney.[130]

V. Pornography and Privacy Rights

The adult entertainment industry in the United States owes much to *Stanley v. Georgia*,[131] the Supreme Court ruling more than four decades ago that holds states may not criminalize the mere private possession of materials deemed by the government to be obscene.[132] Without the ability to possess and use sexually explicit material at home free from the specter of state interference, sales of pornographic videotapes, and eventually DVDs and content transmitted over the Internet, likely would have been (unlike the activities they depict) seriously inhibited. The case arose when law enforcement officers searching Robert Eli Stanley's home for evidence of bookmaking found several film reels in a desk drawer, used Stanley's projector and screen to view them, and determined they were obscene.[133]

The Court held that laws criminalizing the possession of obscenity violate citizens' First Amendment rights to *receive* information, as well as their liberties of thought and expression.[134] Because Stanley was prosecuted for what he kept in a desk drawer away from public view, the Court said, his prosecution also infringed his fundamental right to privacy.[135] The Court said that "in the context of this case—a prosecution for mere possession of printed or filmed matter in the privacy of a person's own home—that right [to receive information] takes on an added dimension. For also *fundamental* is the right to be free, except in very limited circumstances, from unwanted governmental intrusions into one's *privacy*."[136]

---

[130] *Id.*
[131] Stanley v. Georgia, 394 U.S. 557 (1966).
[132] *Id.* at 568.
[133] *Id.* at 558.
[134] *Id.* at 563-65.
[135] *Id.* at 564.
[136] *Id.* (emphasis added).

Stanley was part of the Court's recognition of the sexual dimensions of liberty and privacy beginning in the 1960s that also included rulings such as *Griswold v. Connecticut*[137] and *Eisenstadt v. Baird*,[138] which upheld the rights of heterosexual couples to buy and use contraceptives. Most recently, the Court in *Lawrence v. Texas*[139] cemented the rights of Americans to be free from criminal liability for noncommercial, consensual sexual activity between unrelated adults. [140] The Court held that the "right to liberty under the Due Process Clause gives [citizens] the full right to engage in[homosexual] conduct without intervention of the government."[141]

One common thread running through these decisions is the Court's recognition of constitutionally protected liberties of privacy and autonomy in adults' sexual thoughts, desires, predilections, and consensual activities.[142] Although the Court's jurisprudence on broader informational privacy rights is quite opaque,[143] its interpretation of the right to sexual privacy is clearer. The Court held in *Lawrence*, for example, that the Texas law criminalizing sex acts between people of the same gender "furthers no legitimate state interest which can justify its *intrusion into the personal and private life* of the individual."[144] To be sure, *Lawrence* has confused and frustrated some courts and commentators because—as eagerly pointed out by

[137] Griswold v. Connecticut, 381 U.S. 479 (1965).
[138] Eisenstadt v. Baird, 405 U.S. 438 (1972).
[139] Lawrence v. Texas, 539 U.S. 558 (2003).
[140] *Id.* at 578-79.
[141] *Id.*
[142] *See, e.g.*, *id* at 578 ("The state cannot demean [gays'] existence or control their destiny by making their private sexual conduct a crime."); *Stanley*, 394 U.S. at 564.
[143] The Court in *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977) and *Nixon v. Administrator of General Services*, 433 U.S. 425, 457 (1977) seemed to recognize, in *dicta*, a constitutional right to informational privacy that protects against disclosure of personal information such as medical records. The Court recently acknowledged that most federal circuits have interpreted *Whalen* and *Nixon* as, at a minimum, recognizing a constitutional privacy interest requiring balancing against the governmental interests in such disclosures. National Aeronautics & Space Administration v. Nelson, --- U.S. ---, 131 S.Ct. 746, 756 & n.9 (2011). However, the Court refused to clear up the ambiguity, pointedly rejecting calls by two concurring justices for a definitive holding and explaining that the Court "decide[s] the case before us and leaves broader issues for another day." *Id.* at 757 & n.10.
[144] *Lawrence*, 539 U.S. at 578 (emphasis added).

Justice Scalia's dissent[145]—it does not speak the same language of fundamental rights most often used in substantive due process jurisprudence or explicitly apply heightened scrutiny.[146] But the constitutional protections for sexual privacy recognized in *Lawrence* (not to mention *Stanley, Griswold*, and *Eisenstadt*) are clear, and the majority of federal circuits to consider the question have reaffirmed that the Constitution does protect sexual privacy.[147]

Privacy rights are not absolute, of course; they must be balanced against the governmental interests involved.[148] However, those governmental interests must be "genuine, legitimate, and compelling,"[149] as the Third Circuit put it. For example, a self-insured government employer has a genuine, legitimate and compelling need to obtain and monitor records of the prescriptions filled by employees, even though that information can show that an employee is infected with HIV.[150] Further, "the more intimate or personal the information, the more justified is the expectation that it will not be subject to public scrutiny."[151] Information about one's sexuality is among the most intimate and personal imaginable.[152]

Federal appellate courts, therefore, consistently hold that a person's sexual practices or sexual orientation are especially sensitive matters whose disclosure by the government generally violates constitutionally protected privacy rights.[153] Courts have found privacy violations by

---

[145] *Id.* at 593& n.3 (Scalia, J., dissenting).
[146] *See* Donald H.J. Hermann, *Pulling the Fig Leaf Off of the Right of Privacy: Sex and the Constitution*, 54 DEPAUL L. REV. 909, 946-51 (2005) (discussing and refuting the view that *Lawrence* did not recognize a fundamental right). For a defense of Justice Kennedy's approach in the majority opinion, see Laurence H. Tribe, Lawrence v. Texas*: The 'Fundamental Right' That Dare Not Speak Its Name*, 117 HARV. L. REV. 1893 (2004).
[147] *Compare* Cook v. Gates, 528 F.3d 42, 51-52 (1st Cir. 2008) ("*Lawrence* did indeed recognize a protected liberty interest for adults to engage in private, consensual sexual intimacy") *and* Witt v. Dep't of the Air Force, 527 F.3d 806, 818-19 (9th Cir. 2008) (holding that *Lawrence* requires heightened scrutiny for governmental actions that intrude upon sexual privacy) *and* Reliable Consultants, Inc. v. Earle, 517 F.3d 738, 744-45 & n.32 (5th Cir. 2008) (*Lawrence* protected sexual privacy) *with* Williams v. Attorney Gen. of Alabama, 378 F.3d 1232, 1235-36 (11th Cir. 2004) (holding that no fundamental right to sexual privacy exists and stating that *Lawrence* did not recognize such a fundamental right). Still, even the Eleventh Circuit does not deny that a right to sexual privacy *exists*; it only disputes whether that right is *fundamental. See id.*
[148] *See, e.g.*, U.S. v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980).
[149] Doe v. Se. Pa. Trans. Auth., 72 F.3d 1133, 1141 (3d Cir. 1995).
[150] *Id.*
[151] Sterling v. Borough of Minersville, 232 F.3d 190, 195 (3d Cir. 2000) (quotation and citation omitted).
[152] *Id.* at 196.
[153] *See, e.g., id.*

government actors who disclosed or threatened to disclose information including the identities of the person's sexual partners[154] or that the person is transgendered,[155] for example.

A governmental action outing someone as lesbian, gay, or bisexual is particularly improper, as illustrated by the tragic case of *Sterling v. Borough of Minersville*.[156] There, a police officer arrested18-year-old Marcus Wayman for underage drinking and threatened to tell Wayman's grandfather that Wayman was gay.[157] The young man killed himself shortly after his release from police custody.[158] His mother sued, and the Third Circuit held that the officer's threat to reveal Wayman's sexual orientation had violated the young man's clearly established constitutional rights: "It is difficult to imagine a more private matter than one's sexuality and a less likely probability that the government would have a legitimate interest in disclosure of sexual identity. . . . Wayman's sexual orientation was an intimate aspect of his personality entitled to privacy protection."[159] Federal district courts also frequently hold that disclosure or threats of disclosure of one's status as gay or lesbian is an invasion of privacy.[160]

Being gay is nothing shameful. But sexuality is a deeply personal matter, and it is each individual's choice whether and to what extent to share his or her sexual identity with others. As the *Sterling* case illustrates, governmental action forcing someone out of the closet can be emotionally distressing to the point of suicide. Moreover, open discrimination and social stigma remain stark realities for gays and lesbians in the United States.[161] Given that hate crimes

---

[154] Thorne v. City of El Segundo, 726 F.2d 459, 469-70 (9th Cir. 1983).
[155] Powell v. Schriver, 175 F.3d 107, 111 (2d Cir. 1999).
[156] *Sterling*, 232 F.3d at 192-93.
[157] *Id.* at 193.
[158] *Id.*
[159] *Id.* at 196 (footnote omitted).
[160] *See, e.g.*, Wyatt v. Kilgore Indep. Sch. Dist., No. 6:10-cv-674, 2011 WL 6016467, at *6 (E.D. Tex. Nov. 30, 2011); Nguan v. Wolf, 517 F. Supp. 2d 1177, 1193 (C.D. Cal. 2007); Johnson v. Riggs, No. 03-C-219, 2005 WL 2249874, at *11-12 (E.D. Wis. Sept. 15, 2005).
[161] *See, e.g.*, M.V. Lee Badgett, et al., *Bias in the Workplace: Consistent Evidence of Sexual Orientation and Gender Identity Discrimination 1998-2008*, 84 CHI.-KENT L. REV. 559, 560-61 (2009) (discussing various studies and concluding that "our review of the evidence demonstrates one disturbing and consistent pattern: sexual orientation-based and gender identity discrimination is a common occurrence in many workplaces across the country.").

against those perceived to be lesbian, gay, bisexual or transgender (LGBT) are still far too prevalent,[162] being identified as such can put that person in life-threatening physical danger.

While not as extreme as the open and violent hatred often expressed toward LGBT people, there is also a social stigma attached to pornography.[163] As one commentator put it: "Pornography, despite being legal, is still taboo, and revealing one's use or being caught in possession of pornography can cause embarrassment and shame."[164] That taboo gives the adult entertainment plaintiffs leverage to, in the words of one of those targeted, "embarrass and shame defendants . . . into paying money to avoid being publicly associated with the downloading of pornography over the Internet"[165] because "to be accused of downloading pornography is to be stigmatized and branded in ways which may never be overcome."[166]

At their worst, then, these lawsuits are a frame-and-shame operation in which the threat of publicly (but falsely) accusing the targets of illegally downloading porn is used to intimidate innocent people into making payoffs to avoid humiliation. Even where the allegations are true, the plaintiffs are deliberately leveraging the prospect of being outed—as gay, as an aficionado of certain frowned-upon sexual practices, or simply as someone who enjoys pornography—to extract payments from people who do not want to be publicly labeled as such. Stone, the sanctioned Texas lawyer, bragged about this tactic to Texas Lawyer magazine: "You have people that might be OK purchasing music off iTunes, but they're not OK letting their wife know that

[162] Law enforcement agencies reported to the FBI 1,470 hate crimes based on sexual orientation in 2010. *Hate Crime Statistics 2010: Incidents and Offenses*, FBI CRIM. JUST. INFO. SERVS. DIV., http://www.fbi.gov/about-us/cjis/ucr/hate-crime/2010/narratives/hate-crime-2010-incidents-and-offenses (last visited Apr. 15, 2012).
[163] Tom W. Bell, *Pornography, Privacy, and Digital Self-Help*, 19 J. MARSHALL J. COMPUTER & INFO. L. 133, 133 (2000) ("Pornography tends to generate social stigma.").
[164] Alan James Kluegel, *The Link Between* Carolene Products *and* Griswold*: How the Right to Privacy Protects Popular Practices from Democratic Failures*, 42 U.S.F. L. REV. 715, 730 (2008).
[165] Answer and Counterclaims of Bailey Zwarycz, AKA John Does 116 and 117 at ¶ 29, Third Degree Films, Inc. v. Does 1-152, No. 1:11-cv-01833-BAH (D.D.C. Feb. 1, 2012).
[166] *Id.* at ¶ 30.

they are purchasing pornography."[167] It's not surprising, then, that lawyers for the adult entertainment plaintiffs boast that large numbers of defendants quickly agree to settlements.[168]

Courts should not countenance such invasions of privacy, let alone facilitate them. A person's sexual privacy and autonomy rights are infringed by unjustified, government-sanctioned inquiries into and exposure of individuals' choices (or alleged choices) of sexually explicit materials. Given that a police officer's threat to out a young man as gay is a clear constitutional violation,[169] plaintiffs' threats to use court-approved discovery to similarly identify individuals' intimate sexual information is a privacy invasion of constitutional dimensions. Subpoenas in pornography infringement cases therefore infringe defendants' rights by using the judicial system in threatening to announce (whether truthfully or falsely) that (1) the person's sexual fantasies involve the subject matter of the allegedly infringed work, and (2) the accused individual likes this kind pornography so much he or she is willing to break the law to obtain free copies of it.

Judges, therefore, should consider the harm to the constitutionally protected right to sexual privacy when determining whether to grant subpoenas in copyright infringement cases. Courts have recognized in the defamation context that when constitutional rights are at stake, close scrutiny of plaintiffs' claims is required to ensure with greater certainty that those claims are legitimate.[170] Providing discovery to a civil litigant—particularly in a case the plaintiff is eager to settle for just a few thousand dollars—is not so compelling an interest as to justify invading people's privacy with minimal judicial oversight.

---

[167] John Council, *Adult Film Company's Suit Shows Texas is Good for Copyright Cases*, TEXAS LAWYER (Oct. 4, 2010).
[168] *Id.* (quoting Stone as claiming a 45% settlement rate); Rhett Pardon, *Porn BitTorrent Litigation Getting Trickier, Lawyer Says*, XBIZ.COM (Oct. 14, 2011), http://www.xbiz.com/news/news_piece.php?id=139696&mi=all&q=BitTorrent (quoting adult entertainment industry lawyer's declaration in an infringement case as saying that "in any given joined suit 35-55 percent of the Doe defendants will settle very early in the litigation").
[169] *See* Sterling v. Borough of Minersville, 232 F.3d 190, 192 (3d Cir. 2000).
[170] *See infra* notes 173-178 and accompanying text.

VI. How To Get There From Here: Procedural Issues in John Doe Lawsuits

Courts have three main procedural tools to keep John Doe lawsuits in check. First and most importantly, the plaintiff must persuade the court to approve its subpoenas to the Does' ISPs. If raised by the court at that initial stage, or if raised by putative defendants after the subpoenas have been issued, the plaintiff also must prevail over challenges to personal jurisdiction and venue, and show that joinder is proper. Federal courts presented with these questions have provided widely varying and often contradictory answers.

A. To ID Or Not To ID: The Threshold Question

The first and most fundamental issue in any John Doe lawsuit is what requirements must be met before the court allows the plaintiff to identify the anonymous defendants. Cases in which parties seek court-ordered unmasking of anonymous Internet users necessarily require courts to consider the balance between the plaintiffs' rights to locate and sue alleged wrongdoers and the putative defendants' interrelated rights to privacy, anonymity, and expression. The Supreme Court has not ruled on how courts should set that balance, leaving state and lower federal courts to develop their own standards.[171] Although those standards vary, the case law has largely coalesced around two general approaches: a high-burden test where the online conduct involves expressive speech, such as in cases of alleged defamation; and lower-burden tests for cases alleging copyright or trademark infringement.[172]

The majority view among courts considering attempts to identify anonymous online speakers is that the plaintiff must put forth enough evidence to show that she has a legitimate claim,[173] a test formulated in two slightly different ways in the lead cases on the subject,

[171] Kissinger & Larsen, *Protections*, *supra* note 38, at 826.
[172] *Id.* at 827.
[173] Sinclair v. TubeSockTedD, 596 F. Supp. 2d 128, 132 (D.D.C. 2009) (noting that "two similar standards have emerged in cases involving discovery seeking the identification of anonymous Internet speakers" and that both standards require "an examination of the sufficiency of a plaintiff's claims"); *In re* Indiana Newspapers, Inc., --- N.E.2d ---, 2012 WL 540796, at *13 (Ind. Ct. App.

Dendrite International, Inc. v. Doe No. 3[174] and *Doe v. Cahill*.[175] In *Dendrite*, a New Jersey appellate court held that before an anonymous Internet speaker may be identified, the plaintiff must show that, for each element of her claim, enough evidence exists to show she has a prima facie case.[176] The *Dendrite* test further requires that, if the prima facie standard is met, the trial court must balance the speaker's First Amendment right to anonymous expression against the strength of the plaintiff's case.[177] The Delaware Supreme Court in *Cahill* adopted a modified version of this standard which requires the plaintiff to provide enough evidence to withstand a hypothetical summary judgment motion but does not require an explicit balancing of the competing interests of plaintiff and anonymous speaker.[178]

Courts usually use lower-burden tests in cases of alleged copyright infringement, however, reasoning in part that while infringing file-sharing does have expressive elements, it does not deserve the same degree of First Amendment protection as "pure" speech.[179] Then-U.S. District Judge Denny Chin, for example, wrote that sharing music files "qualifies as speech, but only to a degree," is not "true expression," and therefore its First Amendment protection is limited "and subject to other considerations."[180]

Most courts considering copyright claims, therefore, use some kind of "motion to dismiss" or "good cause" test to determine the validity of a plaintiff's request for discovery to identify the alleged infringers. Judge Chin's decision in *Sony Music Entertainment Inc. v. Does*

Feb. 21, 2012) ("[T]wo relatively similar standards for revealing the identity of an online commenter have emerged as the most commonly used across the country. . . . [A]nd both require that the plaintiff provide some proof of his defamation claim before the anonymous speaker is revealed.").

[174] Dendrite Int'l Inc. v. Doe No. 3, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001).

[175] Doe v. Cahill, 884 A.2d 451 (Del. 2005).

[176] *Dendrite*, 774 A.2d at 760.

[177] *Id.* at 760-61.

[178] *Cahill*, 884 A.2d at 461. The *Cahill* court also explained that the plaintiff need not provide evidence on elements beyond his control, such as the defendant's state of mind. *Id.* at 464.

[179] Sony Music Ent'mt Inc. v. Does 1-40, 326 F.Supp.2d 556, 564 (S.D.N.Y. 2004).

[180] *Id.*

1-40[181] is one of the most influential. The ruling at first glance appears to follow the more stringent *Dendrite* standard by requiring a "concrete showing of a *prima facie* claim of actionable harm."[182] But under the *Sony* formulation, the plaintiff has a much lower burden, and can satisfy the *prima facie* requirement "merely by alleging the elements of ownership and copying in some detail in the complaint."[183]

However, an often-overlooked section of the *Sony* opinion notes that courts should consider defendants' "expectations of privacy."[184] Nevertheless, the opinion holds that online file sharers "have little expectation of privacy in downloading and distributing copyrighted songs without permission" because such activities are prohibited by their ISPs' terms of service, which also state that subscriber information can be disclosed under a subpoena.[185]

Another widely used standard is that laid down by the Northern District of California in an early "cybersquatting" case, *Columbia Insurance Co. v. Seescandy.com*.[186] There, the court held that the plaintiff could obtain a subpoena to identify an infringement defendant if it could "establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss."[187] As with *Sony*, however, this formulation of the test is somewhat misleading. The court went on to hold that the plaintiff must make an evidentiary showing akin to probable cause in the criminal context.[188] As "a protection against the misuse of *ex parte* procedures to invade the privacy of one who has done no wrong," the plaintiff "must make some

[181] Sony Music Ent'mt Inc. v. Does 1-40, 326 F.Supp.2d 556 (S.D.N.Y. 2004).
[182] *Sony*, 326 F. Supp. 2d at 564.
[183] Kissinger & Larsen, *Legal Labyrinth*, *supra* note 40, at 20.
[184] *Id.* at 565.
[185] *Sony*, 326 F. Supp. 2d at 566-67.
[186] Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999). The plaintiff, the assignee of the trademark to the Sees candy store chain, sued to gain control of the domain names seescandy.com and seescandys.com.
[187] *Id.* at 579.
[188] *Id.*

showing that an act giving rise to civil liability actually occurred and that the discovery is aimed at revealing specific identifying features of the person or entity who committed that act."[189]

Some courts in copyright cases have employed an even looser "good cause" standard, essentially requiring nothing more than the showing necessary in other civil actions under Federal Rule of Civil Procedure 26(d).[190] Those courts have reasoned that an enhanced standard is not appropriate where there is no "actual speech" and thus the "defendant's First Amendment privacy interests are exceedingly small."[191] Good cause exists, these courts have said, when there are cognizable allegations of copyright infringement, a danger the ISP will delete the identifying information, and expedited discovery is necessary to move the case forward.[192]

The prospect of copyright holders accusing innocent defendants has prompted some courts in BitTorrent cases to enter protective orders limiting the use and dissemination of the identifying information plaintiffs obtain from ISPs.[193] Those courts have required, for example, that the ISPs not turn over subscribers' telephone numbers and that the ISPs and their subscribers be given 60 days to challenge the subpoenas before the plaintiff can use the identifying information.[194] This procedure is meant to balance the plaintiffs' stated need to obtain the information before it is purged by the ISPs and the countervailing need to avoid undue prejudice to the putative defendants.[195]

---

[189] *Id.* at 579-80.
[190] *See, e.g.*, Arista Records LLC v. Does 1-19, 551 F. Supp. 2d 1, 6 (D.D.C. 2008) (applying good cause standard and collecting cases in which other courts have done so).
[191] *Id.* at 8.
[192] LaFace Records, LLC v. Does 1-5, No. 2:07-CV-187, 2007 WL 2867351, at *1 (W.D. Mich. Sept. 27, 2007).
[193] *See, e.g.*, Hard Drive Prods., Inc. v. Does 1-59, No. H-12-0699, 2012 WL 1096117, at *2-3 (S.D. Tex. Mar. 30, 2012) (ordering that the identifying information sought would be sealed for 60 days for the putative defendants to be notified and given an opportunity to challenge the subpoena); Digital Sin, Inc. v. Does 1-176, No. 12-CV-00126 (AJN), 2012 WL 263491, at *3-4, 6 (S.D.N.Y. Jan. 30, 2012) (same); Digital Sin, Inc. v. Does 1-5,698, No. C 11-04397 LB, 2011 WL 5362068, at *4 (N.D. Cal. Nov. 4, 2011) (entering protective order providing for a 30-day challenge period).
[194] Digital Sin, Inc. v. Does 1-176, No. 12-CV-00126 (AJN), 2012 WL 263491, at *3-4, 6 (S.D.N.Y. Jan. 30, 2012).
[195] *Id.*

Judges who entered protective orders indicated that another reason for doing so was concern about potential defendants' privacy for "matters of a sensitive and highly personal nature, including one's sexuality."[196] In contrast, some judges have brushed aside such privacy concerns and refused to enter protective orders. One explained that "[a]lthough the Court acknowledges that there is some social stigma attached to consuming pornography, Defendant strenuously denies the allegations, and it is the rare civil lawsuit in which a defendant is not accused of behavior of which others may disapprove."[197]

B. Why Are We Here? Jurisdiction and Venue

John Doe lawsuits beg another basic question: If the plaintiff has nothing to identify the defendants other than their IP addresses, how can the court be sure that it has personal jurisdiction over the defendants and venue is proper? Courts have taken sharply divergent paths on this issue, with splits developing even within the same judicial district.

The initial concern is when and by whom these jurisdictional issues can be raised. Some courts more friendly to copyright owners have held that questions of personal jurisdiction and venue are premature when the defendants have not been identified beyond their IP addresses.[198] Courts more skeptical of plaintiffs' claims have held the opposite: without a showing that personal jurisdiction is likely to exist and venue is therefore proper, these courts say, the John Doe cases may not proceed.[199]

---

[196] Digital Sin, Inc. v. Does 1-5,698, No. C 11-04397 LB, 2011 WL 5362068, at *4 (N.D. Cal. Nov. 4, 2011). *See also* Digital Sin, Inc. v. Does 1-176, No. 12-CV-00126 (AJN), 2012 WL 263491, at *3 (S.D.N.Y. Jan. 30, 2012) ("Th[e] risk of false positives gives rise to the potential for coercing unjust settlements from innocent defendants such as individuals who want to avoid the embarrassment of having their names publicly associated with allegations of illegally downloading 'My Little Panties # 2'") (quotation and citation omitted).

[197] Patrick Collins, Inc. v. Does 1-54, No. CV-11-1602-PHX-GMS, 2012 WL 911432, at *4 (D. Ariz. Mar. 19, 2012).

[198] *See, e.g.*, Call of the Wild Movie, LLC v. Does 1-1,062, 770 F. Supp. 2d 332, 345-48 (D.D.C. 2011) (holding that quashing subpoenas would prevent plaintiffs from showing that venue is proper, and that defendants could challenge personal jurisdiction once they are named).

[199] *See, e.g.*, Digiprotect USA Corp. v. Does 1-266, No. 10 Civ. 8759 (TPG), 2011 WL 1466073, at *5 (S.D.N.Y. April 13, 2011) (allowing subpoenas only for information about IP addresses that "correspond to accounts located in New York"); CP Productions, Inc. v. Does 1-300, No. 10 C 6255, 2011 WL 737761, at *1 (N.D. Ill. Feb. 24, 2011) (dismissing case in part because "there is no justification for dragging into an Illinois federal court, on a wholesale basis, a host of unnamed defendants

Those courts more friendly to defendants usually rely on the fact that the approximate physical location (state or metropolitan area) of most IP addresses can be established using the "geolocation" services of free Internet tools or inexpensive databases.[200] Some courts have required plaintiffs to show via geolocation services that the Doe defendants are likely to be located within their districts.[201] Many copyright holders have responded by alleging in their complaints that geolocation information suggests all defendants can be found in that district.[202]

Further, as some courts have pointed out, if there is no personal jurisdiction over the defendant, venue is *per se* improper. Under the Copyright Act, an infringement suit "may be instituted in the district in which the defendant or his agent resides or may be found."[203] Thus, venue is only appropriate where the defendant is subject to the court's personal jurisdiction.[204]

Courts that require geolocation as a basic jurisdictional showing before granting subpoenas say they are concerned not only about adherence to procedural rules and statutory law but also fairness to the putative defendants, who may be pressured to settle merely to avoid litigating in a faraway court.[205] Another judge in the District of Columbia noted that "it is not appropriate, and there is not good cause, to take third-party discovery in this case solely to obtain information that will be used in another lawsuit in a different venue."[206]

---

over whom personal jurisdiction clearly does not exist and—more importantly—as to whom [plaintiff's] counsel could readily have ascertained that fact").

[200] *See, e.g.*, Nu Image Inc. v. Does 1-23,322, 799 F. Supp. 2d 34, 40-41 (D.D.C. 2011).

[201] *See, e.g.*, *id* at 42 (denying plaintiff's motion for discovery and stating the court would entertain subpoena requests "only for IP addresses that Plaintiff has a good faith basis to believe are reasonably likely to correspond to internet accounts located in the District of Columbia").

[202] *See, e.g.*, Third Degree Films, Inc. v. Does 1-108, No. DKC 11-3007, 2012 WL669055, at *1 (D. Md. Feb. 28, 2012) ("By using geo-location technology, which apparently allows a user to correlate an IP address to a physical location, Plaintiff has attempted to limit the Doe Defendants in this case to persons residing within this district.");
Digital Sin, Inc. v. Does 1-176, No. 12-CV-00126 (AJN), 2012 WL 263491, at *1 (S.D.N.Y. Jan. 30, 2012) (noting that plaintiff's complaint alleged that "[p]ublicly available "reverse IP" checks confirmed that all of these addresses very likely belong to individuals located in New York.").

[203] 28 U.S.C. § 1400(a) (2006).

[204] *Nu Image*, 799 F. Supp. 2d at 37-38. *See also* Millenium TGA v. Doe, No. 10 C 5603, 2011 WL 7444064, at *3 (N.D. Ill. Sept. 26, 2011).

[205] *See, e.g.*, *Digiprotect*, 2011 WL 1466073, at *2.

[206] *Nu Image*, 799 F. Supp. 2d at 41.

Some copyright owners have made bold arguments for what amounts to "swarm jurisdiction," claiming that the swarm members acted in concert, and thus a court would have jurisdiction over all members of a swarm wherever any one member of the swarm could be found. One court in the Northern District of Illinois summed up the contention this way: "Because of the size of the BitTorrent swarms and the decentralized nature of the BitTorrent protocol, [plaintiff] alleged that such unlawful distribution of its copyrighted works occurred in *every jurisdiction in the United States*."[207] Carrying this extraordinary argument to its logical conclusion, any BitTorrent user could be sued anywhere, making jurisdictional rules meaningless, as a California magistrate judge pointed out.[208]

C. Making the Cut: Joinder vs. Severance

Some of the sharpest disagreements among courts adjudicating BitTorrent infringement cases involve issues of joinder. Under Federal Rule of Civil Procedure 20(a)(2), courts may allow the joinder of defendants in a single case where the claim arises from "the same transaction, occurrence, or series of transactions or occurrences" and there is a common question of fact or law.[209] Courts "have struggled to uniformly apply [joinder] case law to actions involving the use of BitTorrent technology,"[210] and their opinions have thus gravitated toward opposite poles.

The courts most accommodating to the plaintiffs have held that "swarm joinder" is appropriate because participation in a swarm download makes the defendants participants in the same series of transactions and provides common questions of fact and law involving the use of

[207] First Time Videos, LLC v. Does 1-500, 276 F.R.D. 241, 245 (N.D. Ill. 2011) (emphasis added).
[208] On the Cheap, LLC v. Does 1-5,011, --- F.R.D. --, 2011 WL 4018258, at *4 (N.D. Cal. Sept. 6, 2011).
[209] F. R. Civ. P. 20(a)(2).
[210] Liberty Media Holdings, LLC v. BitTorrent Swarm, --- F.R.D. ---, 2011 WL 5190048, at *2 (S.D. Fla. Nov. 1, 2011).

BitTorrent technology.[211] As described by plaintiffs, the use of BitTorrent software means "[e]ach putative defendant is a possible source for the plaintiffs' motion pictures, and may be responsible for distributing the motion pictures to the other putative defendants, who are also using the same file-sharing protocol to copy the identical copyrighted material."[212] Supporters also say swarm joinder also serves the interests of fairness and judicial economy because otherwise, plaintiffs would be required to burden the court with hundreds or thousands of individual lawsuits.[213] Any misjoined defendants could be severed later, once they are named.[214]

Courts critical of this swarm joinder theory point out that plaintiffs are basing their joinder arguments on either a misunderstanding or misrepresentation of how BitTorrent works in the real world. While it is true that any seed offering a file or peer downloading a file can be a source for others downloading at the same time, this only happens *when those users are online*—and few people leave their computers on and connected all the time.[215] When the swarm participants are alleged to have downloaded their files on dates weeks or months apart, the likelihood that they are sharing with or downloading from any other individual defendant is considerably lessened. In other words, "the initial participants may never overlap with later participants."[216] As one California judge explained:

> The Court cannot conclude that a Doe Defendant who allegedly downloaded or uploaded a portion of the Motion Picture on May 11, 2011, a Doe Defendant who allegedly did the same on August 10, 2011, and over three thousand Doe

[211] *See, e.g.*, Patrick Collins, Inc. v. Does 1-15, No. 11-cv-02164 (CMA) (MJW), 2012 WL 415436, at *2 (D.Colo. Feb. 8, 2012) (holding plaintiff sufficiently alleged defendants engaged in the same series of transactions because the "nature of the BitTorrent protocol requires concerted action by peers in order to disseminate files, such as the Work, and the Doe defendants allegedly engaged in this concerted action by entering and contributing to the same swarm."); Call of the Wild Movie, LLC v. Does 1-1,062, 770 F. Supp. 2d 332, 342-44 (D.D.C. 2011) (same).
[212] *Id.* at 343.
[213] *See, e.g.*, Third Degree Films, Inc. v. Does 1-108, No. DKC 11-3007, 2012 WL669055, at *5 (D. Md. Feb. 28, 2012) (denying motions to quash and observing that "at this stage in the proceedings, there is little to be gained from severing the Doe Defendants, but there are certain efficiencies to be had by retaining them in the same suit.").
[214] *Id.*
[215] Guo, *supra* note 52, at 156-62.
[216] Third Degree Films, Inc. v. Does 1-131, No. 12-108-PHX-JAT, 2012 WL 692993, at *5 (D. Ariz. Mar. 1, 2012).

> Defendants who allegedly did the same in the interim, were engaged in the single transaction or series of closely-related transactions recognized under Rule 20.[217]

More importantly, anti-joinder decisions have argued that joining large numbers of anonymous defendants in the same action severely prejudices those defendants. Simply complying with the requirement that each defendant serve her pleadings on every other defendant could be a crushing burden.[218] These courts also have held that joining scores of defendants for the purpose of coercing settlements from them is improper and in itself justifies severance.[219] Plaintiffs' arguments that they would be unfairly burdened by being forced to file thousands of separate lawsuits receives little sympathy from the anti-joinder courts, because those judges believe that "the potential for coercing unjust settlements from innocent defendants trumps Plaintiff's interest in maintaining low litigation costs."[220]

Anti-joinder courts also assert that judicial efficiency supports severance. Allowing such massive lawsuits to proceed would be "inefficient, chaotic and expensive," a "logistical nightmare"[221] requiring the courts to handle a deluge of different motions from defendants, many of them acting pro se.[222] Indeed, an Arizona judge observed, "scheduling and conducting hearings and discovery disputes among 132 parties would be almost impossible."[223]

Further, these single suits against massive numbers of defendants deprive federal courts of millions of dollars in revenue. If the plaintiffs in the three largest BitTorrent cases had filed individual suits against each defendant, for example, they would have paid $22.2 million in filing fees instead of just $1,050. One judge who ordered hundreds of defendants severed noted that

---

[217] SBO Pictures, Inc. v. Does 1-3,036, No. 11-4220 SC, 2011 WL 6002620, at *3 (N.D. Cal. Nov. 30, 2011).
[218] *See, e.g.*, K-Beech, Inc. v. Does 1-41, No. V-11-46, 2012 WL 773683, at *4-5 (S.D. Tex. Mar. 8, 2012); Liberty Media Holdings, LLC v. BitTorrent Swarm, --- F.R.D. ---, 2011 WL 5190048, at *3 (S.D. Fla. Nov. 1, 2011).
[219] *See, e.g.*, *K-Beech*, 2012 WL 773683, at *5; *SBO Pictures*, 2011 WL 6002620, at *4.
[220] *Id.*
[221] Hard Drive Prods., Inc. v. Does 1-130, No. C-11-3826 DMR, 2011 WL 5573960, at *4 (N.D. Cal. Nov. 16, 2011).
[222] *Id. See also, e.g., K-Beech*, 2012 WL 773683, at *5; Third Degree Films, Inc. v. Does 1-131, No. 12-108-PHX-JAT, 2012 WL 692993, at *6 (D. Ariz. Mar. 1, 2012).
[223] *Id.*.

"[t]he burden [on the court] is further compounded by the fact that the increased work resulting from mass joinder requires no additional payment beyond the one-time $350 filing fee. Plaintiffs therefore in no way compensate financially for this significant drain on judicial resources."[224]

VII. Channeling the Torrent: How Courts Should Respond

Short of drastic changes to copyright law or civil procedure, mass infringement lawsuits against individuals cannot be completely eliminated. Still, there are real problems with coercive settlements and abuse of the legal system, and courts must respond, not only to protect the rights of all Internet users, but also to prevent a backlash against the legitimate enforcement of copyrights. Fortunately, courts already have the tools to rein in the worst excesses of these lawsuits, protect their dockets from being overwhelmed by toxic litigation, and provide greater protections for Internet users without unduly interfering with copyright holders' rights to obtain redress for infringement. By tightening enforcement of procedural requirements and giving greater weight to Internet users' rights to informational and sexual privacy, courts can curb the abuses by making improper tactics more costly to employ and more difficult to conceal.

A. Tighten Standards for Issuing Subpoenas

Courts can crack down on abusive tactics right from the start by tightening the standards they use for determining whether to grant subpoenas for identifying information about holders of the allegedly offending IP addresses. Courts have recognized in other contexts that where First Amendment rights to expressive speech are implicated, plaintiffs should meet a higher burden to obtain subpoenas.[225] Because mass infringement lawsuits involving sexually explicit content

[224] CineTel Films, Inc. v. Does 1-1,052, No. JFM 8:11-CV-02438, 2012 WL 1142272, at *8 n.4 (D. Md. Apr. 4, 2012). *See also* Pac. Century Int'l, Ltd. v. Does 1-37, --- F. Supp. 2d ---, Nos. 12 C 1057, 12 C 1080, 12 C 1083, 12 C 1085, 12 C 1086, 12 C 1088, 2012 WL 1072312, at *5 n.15 (N.D. Ill. Mar. 30, 2012) ("[T]he plaintiffs' tactics deny the federal courts additional revenue from filing fees in the suits that should be filed to obtain the information the plaintiffs desire.").
[225] *See supra* Part VI.A.

implicate not only the defendants' rights to anonymous speech but also their rights to sexual privacy, courts should hold plaintiffs to a higher standard before issuing these subpoenas.

Courts should enforce a *Dendrite*-style, high-burden test when deciding whether to approve identifying subpoenas in mass infringement cases involving pornography or otherwise stigmatizing content. This higher standard is necessary because, although the *expressive* First Amendment rights of alleged copyright infringers are small, their sexual *privacy* interests are strong and deserve heightened protection.[226] To be sure, this standard does make pursuing such infringement lawsuits more difficult and costly, and perhaps some legitimate infringement claims would fail. However, legitimate defamation and other content-related speech torts are just as worthy causes of action as are copyright infringement claims, and defamation plaintiffs' needs for redress must often give way to the broader First Amendment rights of the public at large. The same should be true for copyright infringement claims such as these where the constitutional interests at stake are weightier than the *de minimis* First Amendment rights implicated by other infringement cases such as those involving sharing infringing music files. In developing the judicial doctrine of fair use, courts recognized that a copyright holder's property rights are not absolute and must yield to higher considerations.[227]

Under this stricter standard, courts should require plaintiffs to provide evidence showing a *prima facie* case exists—one that could survive a hypothetical summary judgment motion—for each element of the copyright claim. For the copyright ownership element of the infringement claim, the plaintiff should be required to document that the work has been registered to the plaintiff (or the plaintiff's licensor or predecessor in interest) by the Copyright Office, not just that an application for registration has been filed. This requirement not only satisfies the higher

[226] *See supra* Part V.
[227] *See, e.g.*, Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 575 (1994); Pierre N. Laval, *Toward a Fair Use Standard*, 103 HARV. L. REV. 1105, 1135-36 (1990).

evidentiary burden but provides an additional check against the possibility of plaintiffs misusing the court system to extract settlements for infringing works that are uncopyrightable or whose copyright they do not own.[228] For the copying element of the infringement claim, the plaintiff should be required to show that copying occurred through an affidavit or declaration, rather than just relying on the allegations of the complaint.

Even assuming for the sake of argument that alleged pornography infringers' First Amendment and privacy interests are minimal, they are not zero. Thus, courts unwilling to use this higher standard should at the very least enforce the defendant-protective aspects of the lower *Sony* or *Seescandy* standards, which do not give plaintiffs a blank check to seek subpoenas whenever they allege infringement. *Sony* contemplates that a court should consider the defendants' expectations of privacy.[229] Although *Sony* itself concludes that online file sharers have little legitimate expectation of privacy, because those privacy interests are heightened in cases of stigmatizing material, courts should give more weight to this consideration. Courts using the *Seescandy* standard also must keep in mind that opinion's warning that judges must "protect[] against the misuse of *ex parte* procedures to invade the privacy of one who has done no wrong," and require a more detailed evidentiary showing than the bare allegations of a complaint.[230]

Regardless of what standard courts use to determine whether to issue a subpoena, they should keep closer supervision over the dissemination and use of that information. The courts that have allowed the subpoenas to go forward under protective orders limiting the plaintiff's use of the identifying information have struck the proper balance in cases where such discovery is

[228] This is not a theoretical problem. One plaintiff dropped its lawsuit against 5,865 alleged infringers of the movie *Nude Nuns With Big Guns* when a dispute developed over whether it actually owned or licensed the copyright in that work. David Kravets, Nude Nuns *Mass BitTorrent Lawsuit Killed, Clone Lives On*, WIRED.COM THREAT LEVEL BLOG (May 24, 2011, 5:08 PM), http://www.wired.com/threatlevel/2011/05/nude-nuns-curtains/.
[229] *See supra* notes 184-185 and accompanying text.
[230] Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 579-80 (N.D. Cal. 1999).

allowed.[231] The need for protective orders is particularly great where the putative defendants have strong privacy interests and the possibility of misidentifying innocent individuals is high. Using a protective order does not prejudice the plaintiff unless its true purpose is to strong-arm a maximum number of settlements from alleged infringers as quickly as possible. Given the defendants' privacy interests and the potential, not to mention actual, misuse of this information, courts should require such protective orders whenever stigmatizing material is involved.

B. Enforce Personal Jurisdiction and Venue Requirements

It is axiomatic that courts' power extends only as far as their jurisdiction. Ensuring proper personal jurisdiction and venue is especially critical in mass infringement lawsuits where the plaintiff's goal is to use the court's power to obtain identifying information for and extract settlements from individuals without actually naming them as defendants.[232] Plaintiffs should not be able to evade the Copyright Act's venue requirements.[233] Furthermore, it is unjust in the extreme to allow people to be pressured into settlements as a result of actions by and threats of litigation in a court which has no jurisdiction over them—particularly if the court is hundreds or thousands of miles away. Courts, therefore, should take steps to ensure that a reasonable possibility of jurisdiction exists before approving identification subpoenas.

Many courts have realized and enforced the simplest and cheapest method of assuring reasonable grounds for jurisdiction: geolocation.[234] All courts should require plaintiffs to provide geolocation information indicating that the IP addresses in their complaints are likely to be physically located in their districts. The fact that some plaintiffs have begun providing this

[231] *See supra* notes 193-195 and accompanying text.
[232] *See supra* Part VI.B.
[233] *See id.*
[234] *See supra* notes 200-206 and accompanying text.

information and limiting their defendants to those presumably located within a court's jurisdictional boundaries[235] shows that there is no reason not to make this a requirement.

C. Sever Improperly Joined Defendants

One of the simplest ways courts can restrain questionable mass copyright suits is to make a more rigorous examination of whether joinder is proper and to quickly sever all defendants in those cases where it is not. Rule 20's requirements are called "permissive joinder" for a reason, after all: the rule says defendants "*may*" be joined, not "*shall*" be joined.[236] Although the Supreme Court encourages joinder, courts are under no obligation to allow it. Most courts that have considered the issue have rightfully rejected the "swarm joinder" theory[237] because of its obvious deficiencies.[238] At a minimum, courts should allow joinder only of those IP addresses that the plaintiff can show participated in the same swarm *at the same time*, and thus conceivably could have been acting in concert by exchanging bits of the same file with each other.

Severing defendants has a number of advantages as a method of controlling abusive litigation. By increasing the costs and administrative burdens for the plaintiffs, it removes some of the financial advantages of assembly-line settlement coercion while allowing legitimate litigation to proceed. Requiring the filing of single cases also helps provide the filing fees necessary to partially defray the costs that courts would have to absorb whether they handle one case against 100 defendants or 100 cases against a single defendant each. Focusing on one defendant forces the plaintiff to provide individualized evidence to support its claim and allows the judge to evaluate that evidence on a case-by-case basis rather than in the aggregate against a wide range of factually distinct scenarios.

---

[235] *See supra* note 202 and accompanying text .
[236] F. R. CIV. P. 20(a)(2).
[237] Raw Films, Inc. v. Does 1-32, No. 1:11-CV-2939-TWT, 2011 WL 6840590, at *2 (N.D. Ga. Dec. 29, 2011) ("The swarm joinder theory has been considered by various district courts, the majority of which have rejected it.").
[238] *See supra* notes 215-217 and accompanying text.

The flexibility of the permissive joinder rule also makes it well suited for use by judges who have some concerns about a particular lawsuit but do not wish to (or do not believe they have the grounds to) dismiss the action outright. Judges already have severed defendants in mass copyright cases when they suspected improprieties by the plaintiffs.[239] When judges sense potential problems because of red flags such as inconsistencies in the pleadings, the sexual or otherwise stigmatizing nature of the work involved, or previous misconduct by the plaintiff's counsel, they can—and should—use severance as a method to gain closer oversight of the case and head off potential skullduggery.

More fundamentally, courts should be skeptical of attempts to join huge numbers of defendants in a single action. The idea that more than 20,000 individuals can be properly joined in a single infringement lawsuit is highly implausible, to say the least—and even Judge Beryl Howell, a copyright expert who has strongly supported swarm joinder, has acknowledged that "at some point, the sheer number of putative defendants involved in a single case may necessitate severance."[240] While drawing the line at some arbitrary number is unwise, surely once the tally of defendants reaches well into the hundreds and beyond courts should take a hard look at whether any interests other than the plaintiffs' would be served by joining the defendants.

VIII: Conclusion

Copyright infringement is illegal, and it's wrong. The fact that a legitimately copyrighted work is erotic does not and should not divest its owner of the ability to enforce the copyright against infringers, but neither is a copyright a license to infringe upon other citizens' rights to express themselves, to receive information, and to be let alone. The current wave of

[239] *See supra* notes 218-220 and accompanying text.
[240] Donkeyball Movie, LLC v. Does 1-171, 810 F.Supp.2d 20, 31 (D.D.C. 2011).

infringement litigation by the adult entertainment industry has knocked that balance of rights askew, and federal courts have the responsibility to restore the equilibrium.

By wildly suing John Doe defendants by the thousands and pursuing scorched-earth settlement extraction rather than reasonable litigation, some adult entertainment and independent film companies are endangering the same rights to free speech and sexual privacy that have made their primary business possible. Fortunately, federal courts already have the procedural tools they need to curb the excesses of this flood of litigation and channel it into the boundaries required by a just and rational pursuit of appropriate remedies for the harms caused by actual infringement. Closer oversight of the issuance of identifying subpoenas is necessary in cases involving sexual content to preserve privacy and speech rights from undue intrusion. Jurisdiction, venue, and joinder requirements must be more strictly enforced to ensure due process for both those guilty of infringement and those who are incorrectly accused. With the incentives for abusive litigation lessened, the equipoise of intellectual property rights and rights to expression and privacy can be restored.