# STUDENT WORKS

# RETURN OF THE JOHN DOE: PROTECTING ANONYMOUS DEFENDANTS IN COPYRIGHT INFRINGEMENT ACTIONS

Adam Langston*

## *I. INTRODUCTION*

Sarah Ward, a sixty-six-year-old, retired schoolteacher, was an illegal file-sharer. When she was not listening to Celtic or folk music, she worked through her dyslexia and unfamiliarity with computers to share music by Snoop Dogg and other hip-hop artists through file-sharing programs. Confused? So was Sarah, who was accused of downloading thousands of songs using a program that did not even work on her Macintosh computer. While Sarah had several lawyers in her family to help with her case, "the accusation and threat of heavy penalties" kept her up at night, worrying about people who did not have the resources she had.[1]

Cases like Sarah Ward's were the first copyright infringement suits brought directly against file-sharing software users.[2] Today, these actions usually take the form of a "John Doe" lawsuit—a suit brought against an anonymous defendant, who must be "unmasked" or identified.[3] Copyright owners use Doe suits to challenge the sharing of copyrighted works, which they argue vio-

 Recent Developments Editor 2011–2013, *Stetson Law Review*. J.D. candidate, Stetson University College of Law, 2013; B.A., *magna cum laude*, Stetson University, 2006. The Author would like to thank Paul Sarlo and Professor Louis J. Virelli for their helpful comments on earlier drafts and everyone at *Stetson Law Review* who contributed to the Article.

1. John Schwartz, *The New York Times*, *Business Day*, *Media & Advertising*, *She Says She's No Music Pirate. No Snoop Fan, Either.*, http://www.nytimes.com/2003/09/25/business/media/25TUNE.html?adxnnl=1&adxnnlx=1064504734-mFuZwmBwIJ7lwIY+fsz9jg (Sept. 25, 2003). Sarah had no younger relatives living with her and made only limited use of her computer. *Id.* Both the plaintiff and the Internet Service Provider deny that there was any mistake in the identification process. *Id.*

2. *See* Elec. Frontier Found., RIAA v. The People*: Four Years Later* 7, https://www.eff.org/sites/default/files/filenode/riaa_at_four.pdf (Oct. 31, 2011) (noting that Sarah was accused in the first round of lawsuits).

3. *E.g. London-Sire Recs., Inc. v. Doe 1*, 542 F. Supp. 2d 153 (D. Mass. 2008).

lates their rights in the copyrighted works.[4] But the plaintiff must know who the defendant is to serve him or her with process—so the plaintiff hires a private investigator to find the defendant's Internet-protocol (IP) address.[5] To unmask the defendant behind the IP address, the plaintiff must make an ex parte motion asking a judge to allow expedited discovery, so the plaintiff can serve a subpoena duces tecum on the defendant's Internet Service Provider (ISP).[6] If the judge grants the motion, the ISP provides subscriber records revealing who paid for the Internet connection that was using the IP address at a given time.[7] This reveals the owner of the network, but not necessarily the actual user who was sharing copyrighted files.[8] Still, the plaintiffs use the subscriber records to make settlement demands and sometimes to file suit, though in many cases the plaintiffs seem to avoid further proceedings in court.[9]

Although it appeared that these suits were going to decline after 2008,[10] they have returned with a vengeance—naming record numbers of defendants (including a case against 23,322 alleged sharers of *The Expendables*).[11] This expansion has emphasized problems already evident in Doe suits: misidentification of

4. *See e.g. id.* at 165 (arguing that sharing copyrighted files on the Internet violates the exclusive rights of distribution and reproduction).

5. *See e.g. id.* at 159–160 (discussing the third-party investigator MediaSentry, Inc.). An IP address is an identifying number assigned to a computer by an Internet Service Provider when that computer connects to the Internet. *Id.* at 160. This number is not usually constant per computer but is assigned as needed. *Id.*

6. *See* Fed. R. Civ. P. 26(d)(1) ("A party may not seek discovery from any source before the parties have conferred as required by Rule 26(f), except . . . when authorized by these rules, by stipulation, or by court order."); *e.g. Arista Recs. LLC v. Doe 3*, 604 F.3d 110, 112 (2d Cir. 2010) [hereinafter *Arista II*].

7. *London-Sire*, 542 F. Supp. 2d at 160–161.

8. *See* Ray Beckerman, *How the RIAA Litigation Process Works*, at "Introduction," http://beckermanlegal.com/howriaa.htm (updated Apr. 9, 2008) (noting that these lawsuits target the person who paid for the internet access).

9. *See e.g.* Julie Samuels, Electronic Frontier Foundation, Deeplinks Blog, *Courts Call out Copyright Trolls' Coercive Business Model, Threaten Sanctions*, https://www.eff.org/deeplinks/2011/10/courts-call-out-copyright-trolls-coercive-business (Oct. 5, 2011) (observing that some plaintiffs voluntarily dismiss the case after any response in court).

10. *See* Nate Anderson, *Ars Technica*, *Tech Policy*, *News*, *No More Lawsuits: ISPs to Work with RIAA, Cut off P2P Users*, http://arstechnica.com/tech-policy/news/2008/12/no-more-lawsuits-isps-to-work-with-riaa-cut-off-p2p-users.ars (posted Dec. 19, 2008, 10:55 a.m.) (reporting on the announced end of lawsuits by the Recording Industry Association of America).

11. *Nu Image, Inc. v. Does 1–23,322*, 799 F. Supp. 2d 34, 36 (D.D.C. 2011). These suits are sometimes called "mass copyright" cases. *E.g.* Samuels, *supra* n. 9.

defendants, who may settle anyway to avoid intrusive litigation, and ineffectiveness for copyright holders. Because ISPs only provide plaintiffs with subscriber information, the actual copyright infringer may not be identified. This has resulted in many unlikely defendants, including Sarah Ward, a blind man accused of downloading pornography,[12] a child sued for a book report about Harry Potter,[13] and a defendant who no longer even used the ISP that handed over his information.[14] Yet many defendants decide to accept settlements rather than attempt to prove their innocence to avoid the hassle or embarrassment of a lawsuit.[15] Many others have defaulted or have otherwise been unable to respond to cases in distant jurisdictions.[16] Even copyright holders have been dissatisfied with these suits, which have neither effectively compensated copyright holders nor stopped piracy.[17] These problems and other publicized incidents have created a largely negative outlook toward the suits.[18]

The standard for unmasking these defendants has been kept low in spite of constitutional and procedural protections for anonymity. An early case on Internet unmasking called it an "extraordinary" procedure and required plaintiffs to overcome "safeguards" to use it;[19] however, because of pressure to solve the

12. Ernesto, *TorrentFreak*, *Anti-Piracy Lawyers Accuse Blind Man of Downloading Porn*, http://torrentfreak.com/anti-piracy-lawyers-accuse-blind-man-of-downloading-porn-110809/ (Aug. 9, 2011).

13. Alice Kao, Student Author, RIAA v. Verizon*: Applying the Subpoena Provision of the DMCA*, 19 Berkeley Tech. L.J. 405, 423 (2004). The file that prompted the suit contained the words "Harry Potter," and the investigators likely thought it contained copyrighted material. *Id.*

14. Elec. Frontier Found., *supra* n. 2, at 7. The modem used in the infringement somehow remained registered under his name. *Id*.

15. *See e.g.* Nate Anderson, *Ars Technica*, *Tech Policy*, *News*, *How a Troubled West Virginia Lawyer Foisted a* Teen Anal Nightmare *on the Nation*, http://arstechnica.com/tech-policy/news/2011/09/how-a-troubled-west-virginia-lawyer-foisted-a-nightmare-on-the-nation.ars/3 (posted Sept. 19, 2011, 11:30 p.m.) (reporting on a defense lawyer whose clients were afraid of being associated with the pornographic work they were accused of sharing).

16. Patrick Fogarty, *Major Record Labels and the RIAA: Dinosaurs in a Digital Age?* 9 Hous. Bus. & Tax L.J. 140, 157 (2008).

17. *Id.* at 150 (noting that the suits have been called a "money pit," have not deterred piracy, and have been ignored by pirates).

18. *Id.* at 163–164 (calling the suits a "'costly public relations disaster'" (quoting Anders Bylund, *The Motley Fool*, *Investing Commentary*, *RIAA's Day in Court Nearly Over*, http://www.fool.com/investing/general/2007/09/24/riaas-day-in-court-nearly-over.aspx (Sept. 24, 2007))).

19. *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578–580 (N.D. Cal. 1999).

Internet piracy problem, unmasking is perceived as routine in infringement suits today.[20] While First Amendment protections for anonymous speech exist, most courts are reluctant to use them to protect potential copyright infringers,[21] despite the fact that this allows plaintiffs with weak claims to unmask speakers.[22] Nor do the recent U.S. Supreme Court decisions on pleading, *Bell Atlantic Corp. v. Twombly*[23] and *Ashcroft v. Iqbal*,[24] raise the unmasking burden. Motivated in part by concerns of intrusive discovery, these controversial cases raised the burden for all pleadings, requiring a "plausible" claim for relief based on non-conclusory allegations.[25] Unmasking cases raise similar concerns—anyone the subscriber allowed to use his or her network could have been the copyright infringer, and discovery to find that person could be very intrusive.[26] The currently thin protection is not enough to satisfy public concern, *Twombly* and *Iqbal*, and the First Amendment protection for anonymous speech. Accordingly, this Article proposes that for unmasking standards to comply with the First Amendment, *Iqbal*, and the Federal Rules of Civil Procedure, the standards must require both personal jurisdiction and a plausible basis for relief from the specific defendant to be identified.

Part II of this Article explains the history of file-sharing litigation and how courts have historically balanced the interests of copyright and technology. Part II(A) summarizes the litigation against file-sharing software. Part II(B) explains the end of those suits and the movement to the Digital Millennium Copyright Act (DMCA) subpoenas and then to John Doe suits.

---

20. *See* Fogarty, *supra* n. 16, at 156 (noting that judges routinely grant these motions).

21. *See e.g. Arista II*, 604 F.3d at 118–119, 124 (referencing the First Amendment protection for anonymity but refusing to quash a subpoena).

22. *See Mobilisa, Inc. v. Doe 1*, 170 P.3d 712, 719–720 (Ariz. App. Div. 1 2007) (recognizing that a less stringent standard for balancing an anonymous internet user's right to free speech with the need for discovery has the potential to chill anonymous speech).

23. 550 U.S. 544 (2007).

24. 129 S. Ct. 1937 (2009).

25. *Twombly*, 550 U.S. at 556 (first establishing the plausibility standard); *Iqbal*, 129 S. Ct. at 1950–1951 (elaborating on *Twombly*).

26. *See e.g.* Nate Anderson, *Ars Technica*, *Tech Policy*, *News*, *P2P Lawyer: IP Address Not Enough, Let Me Search All PCs in the House*, http://arst.ch/qsu (posted Sept. 7, 2011, 3:37 p.m.) (reporting on a case where the plaintiff asked for discovery on every computer in the Doe's house).

Part III describes the protections currently in place for anonymous defendants. Part III(A) analyzes the development of unmasking standards in other areas, particularly defamation. Part III(B) examines unmasking standards used in copyright infringement actions and how the standards have been kept weak to allow discovery.

Part IV discusses the U.S. Supreme Court's holdings in *Twombly* and *Iqbal*. Part IV(A) looks into the cases themselves, comparing the two cases, the respective rules, and the underlying policy concerns. Part IV(B) briefly examines courts and commentators' reactions to the cases and will weigh some of their benefits and drawbacks.

Part V argues that the standard for unmasking in copyright infringement is too low and must consider the lack of personal jurisdiction and lack of a plausible basis for relief for a specific defendant in many of these cases. Part V(A) argues that the current standard is inadequate under both the First Amendment and the "good cause" standard of the Federal Rules of Civil Procedure. Part V(B) argues that the jurisdictional requirement in earlier unmasking tests has been diluted out of the test and must be restored. Part V(C) proposes that plaintiffs must be able to plausibly identify a specific defendant in order to comply with both *Iqbal* and the First Amendment. Part V(D) responds to potential objections from plaintiffs in these suits. Finally, the Article concludes in Part VI, which looks toward long-term solutions for piracy that are less distasteful than the John Doe lawsuit.

## *II. THE OPENING SCENE: A HISTORY OF FILE-SHARING LITIGATION*

File-sharing litigation has not always been about Doe suits. Rather, Doe suits are somewhat of a last resort. Record labels and the trade group representing them, the Recording Industry Association of America (RIAA), began by attacking the software itself, Peer-to-Peer (P2P) programs such as Napster.[27] P2P programs enable file-sharing by allowing users to download from any other

27. *See* Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement without Restricting Innovation*, 56 Stan. L. Rev. 1345, 1354, 1366, 1368 (2004) (describing how P2P providers can be held liable for contributory infringement and discussing several suits by the recording industry against P2P providers).

user, rather than just from one central server, making file-sharing easier and faster.[28] The P2P software litigation kicked off an arms race that persists today between copyright owners and file-sharing software.[29] Eventually, this arms race spawned file-sharing protocols that were more difficult to attack legally,[30] requiring copyright owners to find other ways to combat piracy. First, they turned to the DMCA, legislation designed to adapt copyright law to online infringement;[31] however, when the courts shut down the DMCA subpoenas,[32] copyright owners finally turned to Doe suits. The history of this area of law demonstrates the need for balance between the many stakeholders in file-sharing litigation: copyright owners, new technologies, Internet providers, and end users.

### A. Flashback: Suits against File-Sharing Technology

Before individual John Doe suits, there was already a body of caselaw balancing the interests of copyright enforcement with those of new technology. Modern litigation over P2P services is built upon the foundation laid by the U.S. Supreme Court in *Sony Corp. of America v. Universal City Studios, Inc.*,[33] which balanced those same interests. Like courts would later do in the P2P context, the Court in *Sony* was tasked with comparing the benefits of a then-new technology, the Betamax tape recorder, with the

28. *See e.g.* BitTorrent, Inc., *Frequently Asked Questions*, *Concepts*, *What is BitTorrent?* http://www.bittorrent.com/help/faq/concepts (accessed July 22, 2012) (explaining how P2P software BitTorrent works).

29. *See* Bryan H. Choi, Student Author, *The Grokster Dead-End*, 19 Harv. J.L. & Tech. 393, 394, 410 (2006) (discussing the P2P community's reaction to the litigation and describing the fight as a "guerilla movement against copyright owners").

30. *See id.* at 400–409 (describing different tactics the P2P industry has used to avoid liability for copyright infringement).

31. Trevor Cloak, Student Author, *The Digital Titanic: The Sinking of YouTube.com in the DMCA's Safe Harbor*, 60 Vand. L. Rev. 1559, 1561 (2007). Although the DMCA sought to address infringement online, it was written before the rise of Napster and thus predates most public debate on file-sharing. *Id.* (DMCA passed in 1998); Choi, *supra* n. 29, at 395 (Napster launched in 1999).

32. *See e.g. Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229, 1231, 1233 (D.C. Cir. 2003) (holding that the DMCA's subpoena provision does not apply to an ISP acting only as a conduit for communications between internet users, including users sharing P2P files).

33. 464 U.S. 417 (1984).

potential for infringing use of that technology.[34] The balance in *Sony* favored the new technology, holding that the Court should leave weighing the merits of technology to Congress.[35] These protections were then weakened for P2P software.[36] *Sony* and its progeny provoked an arms race between P2P software and the law, which would eventually produce BitTorrent and other legal file-sharing software.[37] At first, the courts struck down P2P software, emphasizing that enforcing copyright against individual infringers on the Internet would be an impossible undertaking.[38] This culminated in the *Grokster* decision,[39] a victory for copyright holders delivered by the U.S. Supreme Court.

### B. Cut to Present Day: Suits against Individuals

Despite the legal victory for copyright holders, *Grokster* did little to slow piracy in the long run because of new P2P software, such as BitTorrent, that evades legal liability through an even more decentralized network.[40] By removing the search feature,[41] relying on external search engines,[42] and promoting legal uses,[43] BitTorrent evades the criteria that caused prior software to fail courts' scrutiny. This allows BitTorrent to avoid not only

34. *Id.* at 420, 442. The Betamax recorder was a videocassette recorder similar to VHS players. *See id.* at 422–423 (describing the capabilities of the Betamax player). VHS drove Betamax players out of the market. Jack Schofield, *The Guardian*, *News*, *Technology*, *Why VHS Was Better than Betamax*, http://www.guardian.co.uk/technology/2003/jan/25/comment.comment (Jan. 24, 2003).

35. *Sony*, 474 U.S. at 456.

36. Lemley & Reese, *supra* n. 27, at 1356, 1366, 1368 (describing how lower court decisions have curtailed *Sony*'s protections); *e.g. A&M Recs., Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

37. *See generally* Choi, *supra* n. 29 (arguing that P2P software's ability to quickly adapt would put it beyond the reach of the law).

38. *MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 928–930 (2005) (stating that "digital distribution of copyrighted material threatens copyright holders as never before"); *In re: Aimster Copy. Litig.*, 334 F.3d 643, 645–646 (7th Cir. 2003) (expressing the hopelessness of suing individuals).

39. 545 U.S. 913.

40. Choi, *supra* n. 29, at 402–406; *see generally* BitTorrent, Inc., *supra* n. 28 (explaining how BitTorrent works).

41. Choi, *supra* n. 29, at 400.

42. *Id.* Popular search engines include isoHunt and The Pirate Bay. *IsoHunt*, http://isohunt.com/ (accessed July 22, 2012); *The Pirate Bay*, http://thepiratebay.se (accessed July 22, 2012).

43. *See e.g.* BitTorrentBlog, *FILM: 'A Lonely Place for Dying' Part One Premieres on BitTorrent*, http://blog.bittorrent.com/2011/07/01/download-a-lonely-place-for-dying/ (July 1, 2011, 10:00 a.m.) (promoting an independent film released through BitTorrent).

knowledge and supervision of users' conduct, but also the intent to promote piracy that was fatal to *Grokster*.[44] Further, because individual users host .torrent files, and there are multiple clients and search engines to use, no single bottleneck can shut down all BitTorrent piracy.[45] The result is software that effectively avoids liability—both by working around the legal standard and by avoiding creating a practical target of suit.[46] To continue fighting piracy, copyright owners first turned to the DMCA, which grants copyright holders subpoena power in certain circumstances;[47] however, when courts found the DMCA subpoenas did not apply to ISPs, who were merely "conduits,"[48] copyright owners began the trend in effect today: the John Doe lawsuit. The DMCA procedure and the Doe suits share many problems: inaccuracy and abuse of the process, invasion of privacy, and inefficiency.

Copyright owners first turned to the DMCA's subpoena power.[49] After the copyright holders send notice to the host of infringing content, the DMCA allows copyright holders to subpoena the "service provider" for information identifying the infringing user.[50] This approach concerned courts and commentators alike.[51] The DMCA subpoenas required only a good-faith belief that the information would reveal the identity of an infringer.[52] Further, evidence of both intentional abuse of the

44. *See* Matthew Helton, Student Author, *Secondary Liability for Copyright Infringement: BitTorrent as a Vehicle for Establishing a New Copyright Definition for Staple Articles of Commerce*, 40 Colum. J.L. & Soc. Probs. 1, 24–29 (2006) (analyzing BitTorrent's potential liability for contributory infringement under the *Sony* and *Grokster* doctrines).

45. Choi, *supra* n. 29, at 405–406. Suing intermediaries may still have benefits because it avoids "suing one's own customers." *Id.* at 406.

46. *Id.* at 405–406.

47. *See generally* 17 U.S.C. § 512(h) (2006) (describing the DMCA subpoena power).

48. *Verizon*, 351 F.3d at 1231.

49. Kao, *supra* n. 13, at 406.

50. 17 U.S.C. § 512(h)(1). A "service provider," as referred to in the DMCA, is not the same as an ISP and in fact does not include ISPs. *Verizon*, 351 F.3d at 1233. If service providers do not comply with the DMCA provisions, they lose their statutorily granted "safe harbor" that protects them from infringement suits. *See generally* 17 U.S.C. § 512 (detailing the safe harbor rules).

51. *See e.g. In re: Charter Commc'ns, Inc., Subp. Enforcement Matter*, 393 F.3d 771, 777–778 (8th Cir. 2005) (commenting without deciding that the DMCA subpoena provision might constitute an unconstitutional invasion of the judiciary power); Kao, *supra* n. 13, at 419–424 (criticizing DMCA subpoenas for invasion of privacy and lack of judicial oversight).

52. 17 U.S.C. § 512(h)(4) (stating that a subpoena is in proper form if the notification satisfies the requirements of subsection (c)(3)(A), which states, among other things, that for a notification to be effective it must include "[a] statement that the complaining party

DMCA procedure and inaccurate subpoena requests emerged, highlighting the need for judicial oversight.[53] Many of these concerns, including concerns of abuse and invasion of privacy, have been noted to carry over into the John Doe lawsuit context.[54] Eventually, courts blocked use of the DMCA subpoenas by holding that they did not apply to ISPs, who were merely "conduits" for the infringing material.[55] The District of Columbia Circuit echoed concerns expressed in *Sony*, noting that courts should not "rewrite the DMCA in order to make it fit a new and unforeseen [I]nternet architecture" without input from Congress.[56] These rulings led content holders to pursue other avenues of enforcement, including John Doe lawsuits.

John Doe suits began as an alternative method of reducing piracy after early recording industry losses in *Grokster*,[57] but the method has not been very successful. One of the primary aims of the lawsuits was to boost legal music sales by discouraging piracy and educating the public.[58] Despite some positive findings, many statistics indicate that piracy has held steady or has actually risen.[59] Further, the lawsuit campaign appeared to be expensive and did not generate enough money to pay for its costs.[60] Apparently discouraged, the RIAA decided to stop filing lawsuits and pursue other solutions.[61] In the wake of the RIAA campaign, other

---

has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law"); Kao, *supra* n. 13, at 424.

53. Kao, *supra* n. 13, at 422–424 (listing examples of abuse).

54. *Id.* at 424 (noting that "John Doe lawsuits, while an improvement in many respects over the subpoena provisions, may still be used abusively in ways that are invasive of users' rights of privacy and anonymity").

55. *Charter*, 393 F.3d at 776–777; *Verizon*, 351 F.3d at 1231, 1233.

56. *Verizon*, 351 F.3d at 1238.

57. *See generally MGM Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp. 2d 1029 (C.D. Cal. 2003) (ruling for Grokster in 2003, the same year individual suits began).

58. *See* Recording Indus. Ass'n of Am., *RIAA, Resources, Student FAQ*, http://www.riaa.com/toolsforparents.php?content_selector=resources-for-students (accessed July 22, 2012) (explaining the purpose of the RIAA litigation campaign).

59. *Compare id.* (claiming a reduction in file-sharing) *with* Elec. Frontier Found., *supra* n. 2, at 11–13 (claiming a rise in file-sharing). Despite claims that the suits deter piracy, the RIAA continues to claim a forty-seven percent reduction in sales from piracy. Recording Indus. Ass'n of Am., *supra* n. 58.

60. Fogarty, *supra* n. 16, at 150 (noting that Sony BMG's head of litigation finds the lawsuits a waste of money).

61. Anderson, *supra* n. 10 (noting the end of RIAA's litigation strategy and discussing "graduated response" agreements the RIAA has signed with major ISPs); *see also* Recording Indus. Ass'n of Am., *Senate Introduces PROTECT IP Legislation to Confront Foreign Counterfeiting Websites*, http://riaa.com/newsitem.php?content_selector=newsandviews

groups have tried similar strategies with larger numbers of defendants.[62] While it may be too soon to judge how profitable this strategy is, it appears to be based on harassing and pressuring defendants into settling without any court proceedings.[63] This suggests that any success to be had from Doe suits will be mostly outside of the full legal process.

Additionally, both waves of Doe suits have generated public anger because the damages are excessive, the allegations are not always true, and defendants cannot afford to fight the suits.[64] Many see the suits as the entertainment industries aggressively attacking their own customers,[65] with high statutory damages that are viewed as unfair—tens or even hundreds of thousands of dollars for a heavy user.[66] Critics challenge the accuracy of the allegations, publishing lists of those falsely accused.[67] Others have demonstrated ways that tracking can return a false positive, either by mistake or by reading a disguised IP address.[68] Yet critics claim that the cost of defending the suit and the potential for a high penalty lead even the innocent defendants to settle early.[69] Some even suspect that groups are purposefully bringing suits for

---

&news_month_filter=5&news_year_filter=2011&id=CA760710-42DA-C51C-CC87-D924608F7ACB (May 2011) (press release indicating RIAA's support for anti-piracy legislation); *but see* Nate Anderson, *Ars Technica*, *Tech Policy*, *News*, *AT&T Wants 3 Strikes Tribunal, Government Website Black-list*, http://arstechnica.com/tech-policy/news/2010/04/att-calls-for-us-3-strikes-tribunal-web-censorship.ars (Apr. 30, 2010, 2:20 p.m.) (noting AT&T's resistance to a proposed graduated-response agreement).

62. *E.g.* Jacqui Cheng, *Ars Technica*, *Tech Policy*, *News*, Hurt Locker *Torrenters: Prepare to Get Sued*, http://arstechnica.com/tech-policy/news/2010/05/hurt-locker-torrenters-prepare-to-be-sued.ars (May 12, 2010, 5:42 p.m.).

63. *See* Samuels, *supra* n. 9 (calling these suits "a shakedown scheme").

64. *See* Elec. Frontier Found., *supra* n. 2, at 6–9 (detailing the many problems with the RIAA's use of John Doe suits).

65. *See id.* at 2, 4 (noting that the lawsuit campaign was aimed at the record industry's consumers and that some felt it amounted to extortion).

66. Lemley & Reese, *supra* n. 27, at 1395–1396 (estimating that large uploaders could face "tens of millions of dollars" in damages). These damages have also been (humorously) criticized for not accurately reflecting copyright holders' injuries. *See* Rob Reid, *YouTube*, *Rob Reid: The $8 Billion iPod* at 3:31 to 4:33 (TED Confs. posted Mar. 15, 2012) (available at http://www.youtube.com/watch?v=GZadCj8O1-0) (satirizing the maximum statutory penalty by explaining how the penalty would value MP3 players full of infringing music).

67. Elec. Frontier Found., *supra* n. 2, at 6–7.

68. *See generally* Michael Piatek, Tadayoshi Kohno & Arvind Krishnamurthy, *Challenges and Directions for Monitoring P2P File Sharing Networks—or—Why My Printer Received a DMCA Takedown Notice*, U. of Wash. Technical Rpt., UW-CSE-08-06-01 (June 9, 2008) (available at dmca.cs.washington.edu/uwcse_dmca_tr.pdf) (describing a study that generated many DMCA complaints for innocent IP addresses).

69. Elec. Frontier Found., *supra* n. 2, at 6.

infringement of pornographic videos to encourage defendants to settle rather than risk public embarrassment.[70] ISPs have criticized the large number of IP-address lookup requests, which strains their small subpoena-compliance teams.[71] Overall, critics feel that this litigation unfairly singles out random defendants, many of whom may be innocent, and punishes them with an amount they neither deserve nor can afford to pay.

## *III. THE SET: CURRENT PROTECTIONS FOR ANONYMOUS SPEAKERS*

The courts are left with a question: when should these subpoenas be granted? The content providers find expedited discovery justified under the Federal Rules of Civil Procedure, which allow pre-service discovery if authorized by a judge for good cause.[72] Many defendants have objected, arguing that the subpoenas are an invasion of privacy.[73] Several constitutional objections have been raised, including claims that the high damages violate due process.[74] A common argument concerns the weight of the First Amendment right to anonymity.[75] The First Amendment gives substantial protection to anonymity in other contexts, but many courts have discounted these protections in copyright infringement actions.[76] This has led to a range of "unmasking

70. Nate Anderson, *Ars Technica*, *Tech Policy*, *News*, *Judge Furious at "Inexcusable" P2P Lawyering, Nukes Subpoenas*, http://arstechnica.com/tech-policy/news/2011/06/judge-furious-at-inexcusable-p2p-lawyering-cancels-subpoenas.ars (June 9, 2011, 3:41 p.m. EDT).

71. Nate Anderson, *Ars Technica*, *Tech Policy*, *News*, *Time Warner Cable Tries to Put Brakes on Massive Piracy Case*, http://arstechnica.com/tech-policy/news/2010/05/time-warner-cable-tries-to-put-brakes-on-massive-piracy-case.ars (May 15, 2010, 9:16 p.m. EDT).

72. Fed. R. Civ. P. 26(b)(1), (d)(1). Discovery is also authorized by stipulation. *Id.*

73. *See e.g. London-Sire*, 542 F. Supp. 2d at 179 (discussing a Doe defendant's expectations of privacy).

74. *See generally* Def.'s Opposition to Pls.' Mot. to Dismiss Counterclaims, *Capitol Recs., Inc. v. Alaujan*, 2008 WL 5129583 at pt. II(c) (D. Mass. Oct. 27, 2008) (Nos. 03-CV-11661-NG, 1:07-cv-11446-NG) (arguing that damages authorized by the Digital Theft Deterrence and Copyright Damages Improvement Act of 1999 for file-sharing are so grossly excessive that they violate due process).

75. *See e.g.* Matthew Mazzotta, Student Author, *Balancing Act: Finding Consensus on Standards for Unmasking Anonymous Internet Speakers*, 51 B.C. L. Rev. 833, 833–835 (2010) (discussing the First Amendment right to anonymous speech and the issues surrounding unmasking of Internet speakers).

76. *E.g. Sony Music Entm't, Inc. v. Does 1–40*, 326 F. Supp. 2d 556, 564 (S.D.N.Y. 2004).

standards" for determining when a plaintiff may subpoena a defendant's identity.[77]

### A. A Green-Screen Backdrop: Shifting Standards for Different Claims

First Amendment protections for anonymous defendants fit into a wider right to speak anonymously. Although the original U.S. Supreme Court's holding on anonymous speech concerned the distribution of unsigned pamphlets, the First Amendment extends to the Internet in full.[78] Anonymous speech rights later became an issue in defamation claims, and courts generated a number of tests to determine when it was appropriate to unmask an anonymous defamation defendant.[79] The resulting cases highlight the need to avoid the chilling effects caused by unmasking anonymous speakers.[80]

The right to anonymous speech originated in *McIntyre v. Ohio Elections Commission*,[81] which praised the historical and literary significance of anonymous speech.[82] The Court stressed a speaker's interest in avoiding retaliation, noting, "[a]nonymity is a shield from the tyranny of the majority."[83] The Court recognized that American society values free speech more than it fears its misuse but also noted that the right to remain anonymous is abused when it protects illegal conduct.[84] The opinion referred to the prevalence of anonymous speech throughout history, as used by several noted writers and historical figures.[85] "[A]t least in the

77. Mazzotta, *supra* n. 75, at 855 (noting considerable disagreement on unmasking standards).

78. *Reno v. ACLU*, 521 U.S. 844, 870 (1997) (finding "no basis for qualifying the level of First Amendment scrutiny that should be applied to" the Internet).

79. *See generally* Ashley I. Kissinger & Katharine Larsen, *Untangling the Legal Labyrinth: Protections for Anonymous Online Speech*, 13 J. Internet L. 1 (Mar. 2010) (explaining multiple unmasking tests).

80. *See e.g. Doe No. 1 v. Cahill*, 884 A.2d 451, 457 (Del. 2005) (expressing "concern[ ] that setting the standard too low will chill potential posters from exercising their First Amendment right to speak anonymously").

81. 514 U.S. 334 (1995).

82. *Id.* at 341–343. The Court determined that an Ohio law forbidding anonymous campaign literature was unconstitutional. *Id.* at 336, 357.

83. *Id.* at 357.

84. *Id.*

85. *Id.* at 341–343, 341 n. 4. The Court referenced famous writers who used pseudonyms such as Mark Twain, O. Henry, and Voltaire, as well as historical anonymous publications like the Federalist Papers. *Id.* at 341 n. 4.

field of literary endeavor," the Court concluded, "the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry."[86]

Anonymous defamation cases have embraced this right to prevent a chilling effect on anonymous speech. Two primary tests have emerged in this area: the *Cahill* summary-judgment test[87] and the *Dendrite International, Inc. v. Doe*[88] prima-facie-claim test.[89] While there are some fine differences, the key to both tests is the requirement that the plaintiff meet a summary-judgment-like standard.[90] The *Cahill* court recognized that the unmasking itself was often the primary goal, and a lower test, such as a motion to dismiss, would enable even meritless claims to meet that goal.[91] Being unmasked would open the defendant up to "extra-judicial self-help remedies," such as social ostracism or unwanted exposure—which could compel Internet speakers into self-censorship.[92] The *Dendrite* court similarly expressed concerns about harassment, intimidation, and a chilling effect on Internet speech.[93]

In *Mobilisa, Inc. v. Doe 1*,[94] the Arizona Court of Appeals required any subpoena for the identification of a party (regardless of the type of claim or who the party was) to pass the *Dendrite*

86. *Id.* at 342.

87. 884 A.2d at 460–461.

88. 775 A.2d 756 (N.J. Super. App. Div. 2001).

89. *Id.* at 760–761. Because these tests are inconsistently named, there is some confusion over which tests are similar. *See* Erik P. Lewis, Student Author, *Unmasking "Anon12345": Applying an Appropriate Standard When Private Citizens Seek the Identity of Anonymous Internet Defamation Defendants*, 2009 U. Ill. L. Rev. 947, 955 (classifying *Dendrite* with the motion-to-dismiss test). Similarly, the Southern District of New York uses "prima facie claim" to describe its test but grants the plaintiff's motion much more readily than the *Dendrite* standard would. *Sony Music*, 326 F. Supp. 2d at 565–566 (describing test as a "prima facie claim" but analyzing it in terms of what was "adequately pled").

90. *Cahill*, 884 A.2d at 460–461; *Dendrite*, 775 A.2d at 760–761. The main difference is that *Dendrite* requires an extra balancing test, while *Cahill* insists that the substantive defamation law provides such a test. *Cahill*, 884 A.2d at 460–461; *see also* Anthony Ciolli, *Technology Policy, Internet Privacy, and the Federal Rules of Civil Procedure*, 11 Yale J.L. & Tech. 176, 183–184 (2009) (considering *Dendrite* a case that combines the notice and summary judgment requirements of *Cahill* with a balancing test).

91. *Cahill*, 884 A.2d at 457–458.

92. *Id.* at 457.

93. *Dendrite*, 775 A.2d at 771.

94. 170 P.3d 712 (Ariz. App. Div. 1 2007).

test.[95] The court found that regardless of the nature of the claim, "the potential for chilling anonymous speech remains the same."[96] The court worried that differing standards would encourage plaintiffs to frame their cases as "non-defamation claims," which are subject to a lower standard, easing the ability to obtain discovery.[97] Rather, *Mobilisa* held that considerations unique to each claim should be judged in a balancing test, which should balance a "broader range of competing interests."[98] The court likened this test to the standard for judging preliminary injunctions but recognized that anonymous speakers cannot have their anonymity restored if they prevail at trial.[99]

B. Shooting on Location: Protections in Infringement Suits

In the infringement context, two legal standards purport to protect defendants: the First Amendment and Federal Rule of Civil Procedure 26(d). In spite of *Mobilisa*, courts have contrasted copyright infringement cases with other First Amendment decisions, holding that file-sharing is less valuable speech and does not require extensive First Amendment protection.[100] Rather than apply a test similar to that used for summary judgment, courts tend to apply a test closer to a motion-to-dismiss standard.[101] Other courts give even less protection, finding no First Amendment protection and merely requiring "good cause" under Rule

95. *Id.* at 720.

96. *Id.* at 719. Given the facts of *Mobilisa*, it is easy to see why the court reached this conclusion. While the plaintiffs in *Mobilisa* brought suit for trespass to chattel and violations of electronic communications laws, the real issue seemed to be that the defendant had anonymously forwarded private, personal emails to workers at Mobilisa. *See id.* at 715–716 (describing the facts of *Mobilisa*).

97. *Id.* at 719.

98. *Id.* at 720. The court was not clear as to whether this balancing test was intended to deviate from the balancing test in *Dendrite*, but the court rejected *Cahill*'s argument that this standard is built into the summary-judgment test. *Id.*

99. *Id.* at 721.

100. *See e.g. Sony Music*, 326 F. Supp. 2d at 564 (noting that First Amendment protection for anonymity in a copyright infringement action "is limited, and is subject to other considerations").

101. *See e.g. id.* at 565–566 (analyzing what was "adequately pled").

26(d).[102] Either standard presents a low burden, leading to judges almost routinely granting motions.[103]

The caselaw for copyright infringement draws heavily on a trademark infringement case, *Columbia Insurance Co. v. Seescandy.com*,[104] one of the first cases to adopt a motion-to-dismiss test.[105] Even though it adopted this lower standard, the court expressed concerns similar to *Cahill*, adopting several safeguards to "prevent use of this method to harass or intimidate."[106] Under *Seescandy.com*, a plaintiff must: (1) identify the party "with sufficient specificity" to ensure jurisdiction is satisfied; (2) make a good-faith effort to locate the defendant; and (3) prove to the court that the case "could withstand a motion to dismiss."[107] "A conclusory pleading," however, "will never be sufficient" to pass the motion-to-dismiss test.[108] Although commentators have characterized *Seescandy.com* as a low barrier,[109] a relatively strong amount of evidence supported the decision compared to later cases. The plaintiffs presented substantial evidence to support each of the court's requirements, including email conversa- conversations with a likely zip code for, and possible aliases of, the defendant.[110] Overall, the court noted this procedure was rare, given courts' general reluctance to permit anonymous proceedings.[111]

---

102. *E.g. Arista Recs., LLC v. Does 1–19*, 551 F. Supp. 2d 1, 6–7 (D.D.C. 2008) [hereinafter *Arista I*].

103. *See* Fogarty, *supra* n. 16, at 156, 160–163 (noting that motions have been routinely granted, but also noting some emerging issues).

104. 185 F.R.D. 573 (N.D. Cal. 1999).

105. Ciolli, *supra* n. 90, at 179–180. The *Seescandy.com* court was actually one of the first courts to consider anonymous defendants in any context. *Id.* at 179.

106. *Compare Seescandy.com*, 185 F.R.D. at 578 *with Cahill*, 884 A.2d at 457 (both concerned with extra-judicial harassment).

107. *Seescandy.com*, 185 F.R.D. at 578–580.

108. *Id.* at 579; *see also Iqbal*, 129 S. Ct. at 1949–1950 (discussing the insufficiency of legal conclusions). *Seescandy.com* was decided in 1999 before *Iqbal* was decided in 2009, but the similar language is notable.

109. Ciolli, *supra* n. 90, at 179 (describing the *Seescandy.com* test as "making it very easy to use the discovery process").

110. 185 F.R.D. at 578–580. The defendant had registered a domain name ("www.seescandy.com") that infringed on the plaintiffs' trademarks, and the plaintiffs obtained information on the defendant through the Domain Name System. *Id.* at 575–576. The court was also able to describe how the plaintiffs obtained this information. *Id.*

111. *See id.* at 578–579 (noting the "traditional reluctance" toward the "unusual" and "extraordinary application of the discovery process").

Conversely, when another court applied similar principles to a copyright claim in *Sony Music Entertainment Inc. v. Does 1–40*,[112] it allowed discovery based on very little factual information, analyzing "factors" rather than requiring plaintiffs to overcome "safeguards."[113] In addition to a motion-to-dismiss test,[114] *Sony Music* considered several other factors: the specificity of the request, alternative means to obtain the information, the central need for the information, and the defendants' expectations of privacy.[115] The court further considered the defendants' objections based on improper personal jurisdiction and joinder, both of which it denied.[116] The court ultimately allowed discovery.[117]

The adopted standard appears similar to *Seescandy.com*, but the analysis in *Sony Music* scrutinized the plaintiff's motion far less harshly. The plaintiff in *Seescandy.com* had substantial factual and evidentiary support,[118] but the *Sony Music* court referenced only a declaration by the RIAA vice president for legal affairs as sufficient evidence.[119] The *Sony Music* complaint only alleged that the "[p]laintiffs are informed and believe" that the defendants infringed the copyrights of a list of songs.[120] The court explicitly rejected that any further "sufficient factual showing" was needed.[121] Further, *Sony Music* weakened other elements of the *Seescandy.com* test. While *Seescandy.com* required enough

112. 326 F. Supp. 2d 556 (S.D.N.Y. 2004).

113. *Compare id.* at 564–565, 567 ("does not bar," "factors to weigh," and "right to use the judicial process") *with Seescandy.com*, 185 F.R.D. at 578–580 ("limiting principals," "safeguards," and "requirement[s]").

114. As discussed *supra* note 89, while the *Sony Music* test identifies as a prima-facie-claim test, it appears to actually be a motion-to-dismiss test. *See* Kissinger & Larsen, *supra* n. 79, at 20 (noting that while *Sony Music* appears more protective than *Seescandy.com*, it is actually less protective).

115. *Sony Music*, 326 F. Supp. 2d at 566–567.

116. *Id.* at 567–568. The court denied the personal jurisdiction argument as premature and did not consider joinder because the remedy would be severance, not quashing the subpoena at issue. *Id.*

117. *Id.* at 568. Technically, the court had already allowed discovery but had not considered earlier motions to quash. *Id.* at 561. The motion, if granted, would have returned the information to the ISP. *Id.*

118. 185 F.R.D. at 578–580.

119. 326 F. Supp. 2d at 558 n. 1, 565–566.

120. Compl. for Copy. Infringement, *Sony Music Entm't Inc. v. Does 1–40*, 2004 WL 1432160 at ¶ 25 (S.D.N.Y. Jan. 21, 2004) (No. 04 CV 00473). The complaint attached a list of the songs, but it provided no other allegations tending to suggest that the subscriber paying for the IP address listed was responsible. *Id.*

121. *Sony Music*, 326 F. Supp. 2d at 568 (holding that it will not reconsider its earlier ex parte order allowing expedited discovery).

specificity in the complaint to determine that jurisdiction was proper,[122] *Sony Music* rejected arguments that the court did not have jurisdiction over many of the defendants.[123] Although the court in *Seescandy.com* saw pre-service subpoenas as an "extraordinary" process,[124] the *Sony Music* opinion appears to suggest that copyright holders are *entitled* to pre-service subpoenas unless the defendants can overcome that presumption.[125]

In other cases, many courts have gone even further and required only a showing of good cause.[126] This standard is consistent with the general rule provided in the Federal Rules of Civil Procedure[127] but makes no allowance for the First Amendment. These courts have essentially decided that the First Amendment provides no protection in an anonymous copyright infringement suit.[128] In these cases, courts have allowed discovery because the case could not proceed without it.[129] Essentially, this approach gives the trial judge a lot of discretion to determine whether to issue subpoenas. Despite the arguments of the First Amendment opinions, many courts have adopted only a good-cause requirement.[130]

Recently, the Second Circuit took up this issue, adopted the *Sony Music* test, and discussed the pleading standard.[131] Aside from being the only federal appellate case to address the issue, *Arista II* is notable because it applied the motion-to-dismiss test after the U.S. Supreme Court decisions in *Twombly* and *Iqbal*.[132] In a situation almost identical to *Sony Music*,[133] the Second Cir-

122. 185 F.R.D. at 578.

123. 326 F. Supp. 2d at 567–568 (rejecting personal jurisdiction arguments as premature).

124. 185 F.R.D. at 579.

125. 326 F. Supp. 2d at 567 (stating that "defendants' First Amendment right to remain anonymous must give way to plaintiffs' right to use the judicial process").

126. *E.g. Arista I*, 551 F. Supp. 2d at 6–7; *see also LaFace Recs., LLC v. Does 1–5*, 2007 WL 2867351 at **1–2 (W.D. Mich. Sept. 27, 2007) (listing cases granting discovery requests under Fed. R. Civ. P. 26(d) upon a showing of good cause).

127. Fed. R. Civ. P. 26(b)(1), (d)(1).

128. *Arista I*, 551 F. Supp. 2d at 8–9.

129. *Id.* at 6.

130. *LaFace*, 2007 WL 2867351 at **1–2 (listing cases).

131. *Arista II*, 604 F.3d at 119.

132. *Id.* at 119–123 (decided in 2010); *see also Iqbal*, 129 S. Ct. 1937 (decided in 2009); *Twombly*, 550 U.S. 544 (decided in 2007).

133. *Arista II*, 604 F.3d at 122. Just as in *Sony Music*, the only evidence the court considered necessary to state a claim was a list of downloaded songs and IP addresses along with a declaration from the RIAA vice president for anti-piracy legal affairs. *Id.*; *see also*

cuit held that such complaints were adequate because a list of songs and IP addresses were sufficient factual support.[134] In addition, the court minimized the impact of *Twombly* and *Iqbal*, emphasizing portions of *Twombly* that indicated that the U.S. Supreme Court was still interpreting Rule 12(b)(6) and not creating a heightened standard.[135] As a result, the court upheld *Sony Music* and rejected the idea that *Twombly* had in any way raised the bar.

## *IV. CASTING CALL: PLAUSIBILITY PLEADING*

*Twombly* and *Iqbal* are important cases for unmasking motions—not only because they interpreted the motion to dismiss, but also because they embodied policies about access to discovery. Despite the *Arista II* court's view, many commentators have seen *Twombly* and *Iqbal* as seismic shifts in pleading jurisprudence.[136] In *Twombly*, the U.S. Supreme Court explicitly revoked the prior prevailing language from *Conley v. Gibson*,[137] the seminal case that had previously defined the motion to dismiss. While the *Arista II* court's holding may be plausible in light of *Twombly*, *Iqbal* foreclosed such a reading of *Twombly*. *Iqbal* not only reiterated the new standard, but it expanded the concept of conclusory allegations—effectively raising the factual burden by eliminating certain factual statements as conclusory. Although the ultimate boundaries of the new standard created by the two cases remain somewhat unclear, *Iqbal* is clearly a step away from notice pleading. Further, *Iqbal* can guide and inform a court's interpretation of the motion-to-dismiss standard from *Seescandy.com*.

---

Compl., *Arista Recs., LLC v. Does 1–16*, 2008 WL 4337339 at *5 (N.D.N.Y. July 17, 2008) (making allegations nearly identical to the allegations in *Sony Music*).

134. *Arista II*, 604 F.3d at 121–122.

135. *Id.* at 119–121 (referencing *Swierkiewicz v. Sorema N.A.*, 534 U.S. 506 (2002)). *Twombly* does preserve this case as good law. 550 U.S. at 569–570 (citing *Swierkiewicz* and upholding it).

136. *See* Elizabeth M. Schneider, *The Changing Shape of Federal Civil Pretrial Practice: The Disparate Impact on Civil Rights and Employment Discrimination Cases*, 158 U. Pa. L. Rev. 517, 527 (2010) (describing *Twombly* as "start[ing] a revolution in pleading").

137. 355 U.S. 41 (1957); *see also* Fed. R. Civ. P. 8(a), 12(b)(6) (rules describing the pleading burden and motions to dismiss for failure to state a claim).

### A. Leading Roles: *Twombly* and *Iqbal*

While *Twombly*, especially in isolation from *Iqbal*, leaves much open for debate, it at least took a broad interpretation of *Conley* off the table and required some factual allegations in the complaint.[138] *Twombly* held that surviving a 12(b)(6) motion requires "enough factual matter (taken as true) to suggest" liability.[139] The "plausibility" standard, the Court held, did not require a judge to determine the chance of a fact being true, but merely required a complaint to have "enough fact to raise a reasonable expectation that discovery will reveal evidence of illegal" conduct.[140] Plausibility was not a return to "heightened fact pleading"; it did not require a plaintiff to allege "specific facts," but rather "only enough facts to state a claim to relief that is plausible on its face."[141] Still, *Twombly* elevated the pleading standard from the literal interpretation of *Conley*, which the Second Circuit had adhered to below.[142] Ultimately, pleading under *Twombly* now seemed to turn in part on a distinction between factual allegations—which are entitled to the presumption of truth—and legal conclusions—which are not.[143]

*Iqbal* took this further by elaborating on the distinction between factual allegations and legal conclusions, expanding legal conclusions to include some factual allegations crafted precisely to match legal elements. *Iqbal* boiled the process down to two essential steps: identifying legal conclusions not entitled to the presumption of truth and then deciding whether the complaint was plausible based on the remaining allegations.[144] Although *Twombly* left room for a narrow interpretation of what a legal

138. *See Twombly*, 550 U.S. at 561–562 (listing sources refusing to take *Conley* literally and criticizing a literal reading of *Conley*).

139. *Id.* at 556.

140. *Id.*

141. *Id.* at 570.

142. *See id.* at 561–562 (describing the literal interpretation of *Conley* and concluding it ran contrary to the doctrine).

143. Schneider, *supra* n. 136, at 530 n. 59 ("The murky distinction between factual and legal allegations in the 12(b)(6) context haunts this decision."); *see generally* Elizabeth Thornburg, *Law, Facts, and Power*, 114 Penn St. L. Rev. Penn Statim 1, 2 (Jan. 20, 2010) (available at http://pennstatelawreview.org/114/114%20Penn%20Statim%201.pdf) (criticizing *Iqbal* for its reliance on an impossible-to-determine law/fact distinction).

144. *Iqbal*, 129 S. Ct. at 1950.

conclusion was,[145] *Iqbal* seemed to allow the concept of a legal conclusion to include mixed statements of law and fact. While the legal conclusion in *Twombly* was a rather vague allegation that failed to give any specifics about what conspiracy occurred,[146] *Iqbal* invalidated allegations of a specific discriminatory plan in a civil rights suit.[147] This suggests that *Iqbal* may be more than a mere law/fact distinction.[148] Rather, *Iqbal* seemed to rest on a standard similar to summary judgment, requiring a judge to test whether a jury could plausibly find that the conclusion was true.[149]

Despite expanding views of the standard, the motivation behind both cases remains consistent: enable judges to dismiss meritless or frivolous claims before they can proceed to expensive and burdensome discovery. The *Twombly* Court first indicated this concern in its description of the standard, noting that it called for enough fact to indicate that "discovery will reveal evidence" of illegality.[150] The Court worried that a plaintiff's ability to take up the defendant's time provoked settlements out of fear of litigation.[151] *Iqbal* expanded the concept in the context of qualified immunity: "Litigation, though necessary to ensure that officials comply with the law, exacts heavy costs in terms of efficiency and expenditure of valuable time and resources . . . ."[152]

145. *See id.*; 129 S. Ct. at 1961 (Souter, J., dissenting) (arguing that *Iqbal*'s plaintiff stated a claim because he did not claim "that Ashcroft and Mueller 'knew of, condoned, and willfully and maliciously agreed to subject' him to a discriminatory practice that is left undefined; his allegation is that 'they knew of, condoned, and willfully and maliciously agreed to subject' him to a *particular*, discrete, discriminatory policy detailed in the complaint" (emphasis added)). Justice Souter wrote the majority opinion in *Twombly*. 550 U.S. at 547. This flip suggests that *Twombly* and *Iqbal* were two separate shifts and not one purposeful movement.

146. *See Twombly*, 550 U.S. at 565 n. 10 (comparing the plaintiff's pleadings with model pleadings and noting they were so vague that they would not even provide notice required under Rule 8).

147. *Iqbal*, 129 S. Ct. at 1961 (Souter, J., dissenting).

148. Kevin M. Clermont, *Three Myths about* Twombly-Iqbal, 45 Wake Forest L. Rev. 1337, 1353–1354 (2010) ("Henceforth, the label 'legal conclusion' will attach to any sort of allegation, legal or factual, that a court can ignore as a matter of law."); *but see* Thornburg, *supra* n. 143, at 4 (noting that anything can be labeled as a conclusion and drawing a line between conclusory and non-conclusory allegations is arbitrary).

149. *See generally* Suja A. Thomas, *The New Summary Judgment Motion: The Motion to Dismiss under* Iqbal *and* Twombly, 14 Lewis & Clark L. Rev. 15, 15 (2010) (arguing that under *Iqbal* and *Twombly*, summary judgment and the motion to dismiss are converging).

150. 550 U.S. at 556.

151. *Id.* at 558.

152. 129 S. Ct. at 1953.

Considering this principle, the *Iqbal* Court suggested that the best gate-keeping mechanism was to not consider conclusory allegations, seemingly those allegations made on information and belief.[153]

### B. Supporting Roles: Reactions to the Cases

Many scholars criticize the two cases on a number of grounds.[154] Critics call the doctrine confusing and vague,[155] and worry that because pleading affects every area of law, the confusion will require massive litigation to untangle.[156] Substantively, scholars criticize *Twombly* and *Iqbal* for excluding cases—particularly in civil rights and employment discrimination—where plaintiffs suffer from information asymmetry and lack access to enough information to plead facts.[157] The cases have also been criticized on Seventh Amendment grounds[158] as a "power grab" by the judiciary[159] and as inspiring denial or "pushback" among the lower courts;[160] however, others have defended the

153. *See* Clermont, *supra* n. 148, at 1355 (arguing that the *Iqbal* standard was tailored to the Court's purpose of knocking out certain allegations).

154. *See* Colin T. Reardon, *Pleading in the Information Age*, 85 N.Y.U. L. Rev. 2170, 2171 n. 3 (2010) (listing articles critical of the cases).

155. *See* Clermont, *supra* n. 148, at 1349 (noting that recalling fact pleading would be more efficient than "wandering in the 'non-conclusory plausibility' bewilderness"); Kendall W. Hannon, Student Author, *Much Ado about* Twombly*? A Study on the Impact of* Bell Atlantic Corp. v. Twombly *on 12(b)(6) Motions*, 83 Notre Dame. L. Rev. 1811, 1814 (2008) (noting that *Twombly* made many judges uncertain and confused); Thornburg, *supra* n. 143, at 2, 4 (arguing that the law/fact distinction necessarily creates unclear doctrine).

156. *See* Kevin M. Clermont & Stephen C. Yeazell, *Inventing Tests, Destabilizing Systems*, 95 Iowa L. Rev. 821, 823–824 (2010) (arguing that the Court should not have revolutionized pleading without warning and debate beforehand); Scott Dodson, *Pleading Standards after* Bell Atlantic Corp. v. Twombly, 93 Va. L. Rev. In Brief 135, 142 (July 9, 2007) (available at http://www.virginialawreview.org/inbrief/2007/07/09/dodson.pdf) (speculating on the amount of litigation that *Twombly* would spawn in order to determine its limits).

157. Arthur Miller, *From* Conley *to* Twombly *to* Iqbal*: A Double Play on the Federal Rules of Civil Procedure*, 60 Duke L.J. 1, 46 (2010); *see also* Hannon, *supra* n. 155, at 1814–1815 (noting a spike in dismissals in civil rights claims); Schneider, *supra* n. 136, at 556 (noting that the cases have a disparate impact on civil rights and employment discrimination cases).

158. *See generally* Suja A. Thomas, *Why the Motion to Dismiss is Now Unconstitutional*, 92 Minn. L. Rev. 1851 (2007) (arguing that *Twombly* violates the Seventh Amendment).

159. Thornburg, *supra* n. 143, at 9.

160. Clermont, *supra* n. 148, at 1347 n. 48. Clermont cites *Arista II* as an example of such a case and writes that courts sometimes directly contradict *Iqbal* by allowing more leeway where allegations "particularly within the defendants' knowledge" are concerned. *Id.*

decisions, suggesting that modern plaintiffs have access to more information before discovery[161] and supporting the need for gate-keeping procedures.[162]

## *V. A NEW SCRIPT: RESTORING AND REEVALUATING UNMASKING STANDARDS*

Despite the criticisms of *Iqbal* as a general motion-to-dismiss standard, a gate-keeping method is needed for unmasking motions because of the potential for (and reports of) abuse of the procedure. The unmasking procedure is flawed because it allows plaintiffs to overcome a privilege by using unsupported allegations, unmasking defendants they would otherwise be unable to identify. Although courts have minimized this flaw, asserting that these copyright claims do not involve expressive speech, if only minimal allegations are required, a plaintiff can bring whatever claim will allow discovery. Further, the unmasking procedure encourages rushed litigation that does not accurately identify defendants, who are then forced to choose between the threat of burdensome litigation to clear their names or paying a settlement. When courts ignore personal jurisdiction or venue, defendants have added difficulty protecting their privilege because of the added expense and inconvenience of communicating objections to a court across the country. Looking back at *Seescandy.com* and *Iqbal*, which anticipated issues involving jurisdiction and weak allegations, can solve these problems. To apply these policies to copyright unmasking actions, courts should require plaintiffs to show both that personal jurisdiction is proper and that the discovery sought is sufficient to plausibly identify a specific file-sharer before granting discovery.

### A. Exposition: File-Sharing Defendants Require Protection

Protections for file-sharing defendants are needed, not only because of First-Amendment concerns, but also because of the

161. *See generally* Reardon, *supra* n. 154 (arguing that the Internet and laws mandating open access to information have given plaintiffs many additional resources they did not have when the Federal Rules of Civil Procedure were passed).

162. Richard A. Epstein, Bell Atlantic v. Twombly*: How Motions to Dismiss Become (Disguised) Summary Judgments*, 25 Wash. U. J.L. & Policy 61, 66–68 (2007).

inaccuracies and potential for abuse in the process. While the First Amendment obviously does not provide a bar to copyright enforcement,[163] *Sony Music* nonetheless recognized that it confers some protection from unmasking.[164] Moreover, other factors not considered by *Sony Music*—abuse of the procedure, misidentification, and the expense involved for misidentified defendants—support additional protections. As recognized in *Mobilisa*, providing such a low bar in one area of the law encourages plaintiffs to bring frivolous claims in order to identify defendants they would not be able to identify otherwise.[165] Misidentification, on the other hand, harms legal Internet users who are easily pressured into paying a settlement because of the cost of defending a suit and the extent of discovery needed to clear their names.[166] While most of these major cases discussed above[167] recognize some First Amendment protections, many district courts have improperly applied only a good-cause standard.[168]

*Sony Music* itself noted that even illegal file-sharing is speech because it expresses taste in music and disapproval of copyright owners.[169] While distinguishing file-sharing from true expression, the court noted that a file-sharer could be "making a statement" by distributing music without a license or could be "expressing himself or herself" by the music chosen.[170] Indeed, some file-sharers go out of their way to indicate that file-sharing is a statement in support of "sharing culture"[171] or in opposition to copyright holders' practices.[172] Still, the First Amendment obvi-

163. *London-Sire*, 542 F. Supp. 2d at 163.

164. 326 F. Supp. 2d at 564–565.

165. 170 P.3d at 719.

166. Elec. Frontier Found., *supra* n. 2, at 7.

167. *Supra* pts. III & IV(A).

168. For more information on these cases, see *supra* notes 126–128 and accompanying text.

169. 326 F. Supp. 2d at 564.

170. *Id.*

171. *See* Ernesto, *TorrentFreak*, *Canadian Politician Starts Movie Torrent Site*, http://torrentfreak.com/canadian-politician-starts-movie-torrent-site-110813/ (Aug. 13, 2011) (reporting on the founder of a file-sharing website who hosted the site in the United States with the view that "they can try to extradite my friends and shut down free speech but new sites, new technologies, and new people will always be right around the corner").

172. *See e.g.* Ernesto, *TorrentFreak*, *Ericsson: File-Sharing Is a Symptom Not the Problem*, http://torrentfreak.com/file-sharing-symptom-not-problem-110629/ (June 29, 2011) (arguing that copyright holders create piracy by using outdated and anti-consumer business models).

ously cannot protect everyone who breaks the law because he or she disagrees with it.[173] While the *Sony Music* rationale may be fairly weak, it still recognizes minimum First Amendment protection.

This protection should be amplified in light of *Mobilisa*'s observation that varying standards encourage pleading of frivolous claims to identify a defendant.[174] A plaintiff with a poor defamation case might try to make a copyright infringement argument just strong enough to get discovery—bringing along all the concerns of chilling speech found in *Mobilisa* and *Cahill*. If the plaintiff's only goal is to identify an anonymous speaker, there is no advantage to any particular cause of action. To this end, an IP address could be masked behind another IP address[175]—allowing less scrupulous plaintiffs to set up an investigation that would enable discovery. Abusive use of such subpoenas is not unheard of (DMCA subpoenas have been used to identify downloaders of gay pornography and blackmail them).[176] And considering the number of early dismissals in these cases, the suits already seem to identify thousands of defendants who will never be tried in the courts that afforded their identification.[177] There is no effective way to remedy discovery based on such a pretext because anonymity cannot be restored once it is taken away.

The misidentification of defendants raises other policy concerns, which could be considered under the good-cause standard. Identifying defendants by IP address has shown potential for inaccuracy—a person identified by an IP address is not, as one court has correctly noted, necessarily the copyright infringer.[178] The person identified is the subscriber who paid an ISP for the Internet connection.[179] Thus, a subpoena might result in a need for additional discovery to determine who the infringer is if the

173. *See e.g. United States v. O'Brien*, 391 U.S. 367, 376–377 (1968) (upholding the conviction of a draft-card burner who argued he could not be punished because burning his draft card was a symbolic protest of the draft).

174. 170 P.3d at 719.

175. Piatek et al., *supra* n. 68, at 3.

176. Kao, *supra* n. 13, at 423.

177. houstonlawy3r, TorrentLawyer, a Cashman Law Firm, PLLC Blog, *Federal Computer Crimes, Thousands of John Doe Defendants Quietly Dismissed!* http://torrentlawyer.wordpress.com/2011/03/18/10000-john-doe-defendants-quietly-dismissed/ (Mar. 18, 2011).

178. *VPR Int'l v. Does 1–1017*, No. 2:11-cv-02068-HAB-DGB, slip op. at 2 (C.D. Ill. Apr. 29, 2011) (available at http://www.scribd.com/doc/54508329/ip-baker#archive).

179. Beckerman, *supra* n. 8, at "Introduction."

subscriber is a business or shares his or her network with other people.[180] An individual may also give access to his or her network to guests. In addition, there are several ways an Internet-connected device can be framed or otherwise mistakenly identified as downloading a BitTorrent file.[181] One civil liberties group has pointed out many instances of mistakenly identified downloaders.[182] While the IP address provides a lead, subscriber records for an IP address alone are uncertain means of identifying the actual infringer.

This kind of misidentification can restrict legal uses of file-sharing software, which, as acknowledged by *Sony Music*, is a form of speech. BitTorrent can be used to distribute open-source software,[183] content that the creators allow to be freely distributed,[184] and public-domain content without paying for servers to host the files.[185] These methods could potentially run into trouble, however, due to misnamed files. In at least one case, a misnamed file turned out to be a pornographic video that became the subject of a Doe suit.[186] Exposing these mistaken downloaders to suits threatens to chill the use of P2P programs, which are a valid (albeit unprofitable) means of publishing music, movies, or text documents. Further, the threat of litigation encourages businesses and universities that provide wireless networks to block file-sharing programs. A few sources cited in this paper could not be accessed using Stetson University College of Law's network, including bittorrent.com.[187] This has a chilling effect on use of

180. *See e.g.* Anderson, *supra* n. 26 (reporting on a case where the plaintiff returned to the court to ask to search every computer in the house).

181. *See generally* Piatek et al., *supra* n. 68 (summarizing a study regarding innocent IP addresses).

182. Elec. Frontier Found., *supra* n. 2, at 7–8.

183. *See e.g. LinuxTracker*, http://linuxtracker.org/ (accessed July 22, 2012) (search engine for locating software torrents for Linux, an open-source operating system).

184. *See e.g.* BitTorrentBlog, *supra* n. 43 (promoting an independent film distributed for free).

185. *See* BitTorrent, Inc., *supra* n. 28 (describing how BitTorrent saves bandwidth).

186. Ernesto, *TorrentFreak*, *U.S. P2P Lawsuit Shows Signs of a 'Pirate Honeypot'*, http://torrentfreak.com/u-s-p2p-lawsuit-shows-signs-of-a-pirate-honeypot-110601/ (June 1, 2011). This particular file was not labeled as a public domain file, but the risk could deter users. *Id.* Intent is not an element of a copyright infringement claim, although it can affect damages. *D.C. Comics, Inc. v. Mini Gift Shop*, 912 F.2d 29, 35 (2d Cir. 1990).

187. The Author assumes this means Stetson blocks BitTorrent itself, but given that the college also blocks computer games and video game consoles, liability may not be the school's only concern when it selects web-access protocols.

programs like BitTorrent—which is legal and is sometimes used as a publication platform for controversial speech[188]—by both discouraging legal use and encouraging barriers to clients.

The cost of defending a suit creates pressure to settle, meaning plaintiffs may be getting settlements from innocent defendants even though the plaintiffs have very weak support for their claims. Extremely high potential damages for copyright infringement, combined with the cost of legal representation, create a naturally strong incentive to settle.[189] These suits burden even misidentified defendants, who need to endure discovery on every computer that uses the network to find the actual infringer.[190] This burden rises to highly questionable levels in suits involving pornography, where potential for embarrassment creates an even higher desire to settle.[191] Some settlement letters capitalize on the desire for early settlement by noting the cost of an attorney, stating that defendants can remain anonymous by settling, and claiming that courts will reject various defenses.[192] The Copyright Act permits granting attorney's fees to the winning party;[193] however, the RIAA has managed to avoid paying attorney's fees in many lawsuits.[194] While allowing subpoenas to issue

188. *See e.g. Wikileaks Document Release: Congressional Reports Service Feb 20*, http://thepiratebay.org/torrent/4713076 (Feb. 8, 2009) (a torrent file used by Wikileaks to distribute thousands of "quasi-secret" Congressional Research Service (CRS) documents and an editorial criticizing the CRS' exemption from the Freedom of Information Act).

189. Elec. Frontier Found., *supra* n. 2, at 7.

190. *See e.g.* Stewart Kellar, Boy Racer v. Does 1–52—*Plaintiff Admits in Court that ISP Info Is Insufficient Proof*, http://www.ettorneyatlaw.com/boy-racer-v-1-52-plaintiff-admits-court-isp-info-insufficient-proof/ (Sept. 6, 2011) (describing case-management conference where plaintiff requested additional pre-service discovery).

191. Anderson, *supra* n. 70 (theorizing that there is a shift in plaintiffs' focus from pursuing those who download traditional movies to going after those who download pornography). Lawyers representing pornography distributors have been accused of capitalizing on defendants' desire to quickly settle cases related to pornography, going as far as to neglect other suits in order to pursue pornography suits. *Id.*

192. *E.g.* Ltr. from John L. Steele, Att'y, Steele Hansmeier, PLLC, *Re:* First Time Videos LLC. v. Does 1–500 at 4–5 (May 16, 2011) (available at http://www.scribd.com/fullscreen/57230736). The letter suggests twice that people who leave their wireless networks unsecured may be liable for infringement that occurs on the networks. *Id.* At the time of writing, only one case has addressed this issue, and its analysis was very cursory. *See Liberty Media Holdings, LLC v. Swarm of Nov. 16, 2010, Sharing Hash File A3E6F65F2E3D672400A5908F64ED55B66A0880B8*, 2011 WL 1597495 at *4 (S.D. Cal. Apr. 26, 2011) (allowing discovery for a complaint including negligence with little discussion).

193. 17 U.S.C. § 505 (2006).

194. Fogarty, *supra* n. 16, at 164–179. Fogarty notes an emerging trend of awarding attorney's fees to falsely identified defendants, but a defendant would have to seek legal

is not necessarily a decision on the merits, like a motion to dismiss, it gives the case immediate settlement value and leads to many settlements—giving issuance of subpoenas an effect similar to that of a decision on the merits.

Conversely, many defendants, possibly presuming their innocence and not wishing to fight a lawsuit filed in a different state, ignore the case—either the initial subpoena or the actual proceeding against them. Many of these Doe cases default.[195] The typically short amount of time defendants have to respond to a subpoena, their lack of knowledge about the case, and the difficulty of quickly finding a lawyer admitted in the proper jurisdiction often result in one-sided litigation.[196] Without a personal jurisdiction requirement, these defendants have no way of controlling where litigation is brought against them. The lack of a personal jurisdiction requirement adds to the First Amendment concerns, lack of specificity in the identification, and chilling of legal file-sharing to create several real concerns about this procedure. Between First Amendment protection and the trial judge's discretion under the good-cause standard, file-sharing defendants should be protected from Doe suits.

### B. The First Twist: Jurisdiction Requirements

Defendants' difficulty in responding to these suits could be aided by a requirement from *Seescandy.com*. *Sony Music* seemed to have dropped this straightforward requirement: that the defendant must be specifically identified to show that he or she meets jurisdictional and venue requirements.[197] While *Sony Music* did allude to this requirement, citing *Seescandy.com*, it appears to have twisted it into a requirement for specificity in the *request*, rather than specificity in the identification.[198] Although it is unclear whether this twist is a misunderstanding, an attempt to condense multiple tests from multiple courts, or a deliberate concession in order to allow discovery, *Sony Music* and *Arista II*

advice to know this. *Id.*

195. *Id.* at 157.

196. *Id.* Fogarty notes that the RIAA is often "the only party that has lawyers in court" as the case moves on. *Id.*

197. *Seescandy.com*, 185 F.R.D. at 578.

198. *See Sony Music*, 326 F. Supp. 2d at 566 (suggesting that specificity in the request is likely to lead to identification of defendants).

effectively alter this requirement in a way that has real implications for file-sharing suits.

Both the standard and the analysis conducted by the Northern District of California in *Seescandy.com* indicate that the specificity test is concerned with more than the scope of the discovery request. When establishing the standard, the court acknowledged that the plaintiff bears the burden of establishing jurisdiction and emphasized that the requirement's purpose is to ensure that the court has jurisdiction over a justiciable suit.[199] Additionally, when applying this standard, the court began by acknowledging that all of the suspected addresses for the defendant were located in Artesia, California, which suggested the court likely had jurisdiction.[200] The court's attention to jurisdiction in describing and applying the standard clearly indicates that jurisdiction should not be waived at this stage of the proceedings.

It is possible to obtain a location from an IP address that is accurate enough for jurisdictional purposes. Internet-based tools exist that allow users to look up the geographic location of an IP address.[201] Although *Sony Music* questioned the accuracy of these tools,[202] even where they are inaccurate, they usually at least identify the user's location to the nearest town or zip code.[203] This is certainly specific enough for personal jurisdiction, which is primarily based at the state level.[204] While this evidence may not sufficiently establish jurisdiction in a case on the merits, that level of certainty is not necessary for an unmasking motion. At this early stage, plaintiffs do not have enough information to make detailed personal jurisdiction arguments, but plaintiffs should at least be held to the minimal requirement of using freely available sources to locate a court that has the power to

199. *Seescandy.com*, 185 F.R.D. at 578.

200. *Id.* at 579. The plaintiffs had obtained addresses for the defendant from the domain name service listing. *Id.* at 576. While these addresses were apparently complete enough to pin the defendant down to this area, the plaintiffs could not successfully serve him. *Id.* at 579.

201. *Sony Music*, 326 F. Supp. 2d at 567–568 (rejecting the Doe defendant's suggestion that the plaintiff use these tools and denying a motion to quash based on lack of personal jurisdiction).

202. *Id.*

203. *Nu Image*, 799 F. Supp. 2d at 40–41.

204. *See e.g. Int'l Shoe Co. v. Wash.*, 326 U.S. 310, 311 (1945) (asking whether defendant was subject to proceedings "in the courts of that state").

determine the defendants' rights. To do anything less would be to give plaintiffs complete power to forum shop and file suit in any court they wish.

Most file-sharing suits give plaintiffs free reign.[205] Usually, the question of jurisdiction is delayed until after the defendants are identified.[206] In *Sony Music*, for example, the court refused to consider personal jurisdiction because it could not examine the defendants' contacts with the forum state at that stage.[207] The court seemed to dismiss any possible relevance of the ability to geographically locate an IP address, noting that the location was only "likely" to be correct.[208] This decision effectively reverses the *Seescandy.com* requirement. Instead of placing the burden on the plaintiff to provide jurisdiction, the court actually rejected the defendants' arguments without any supporting allegations or evidence from plaintiffs. Other courts have justified delaying the issue of jurisdiction on grounds of jurisdictional discovery.[209] This flies in the face of requirements that jurisdictional discovery be based on at least a good-faith belief in jurisdiction.[210] In order to protect each defendant's interest in a fair and convenient forum, courts should insist on at least this minimal requirement.

### C. The Climax: *Twombly*, *Iqbal*, and the Plausibility Standard

Considering *Mobilisa* and misidentification issues, *Arista II* misapplied the motion-to-dismiss test under *Seescandy.com* and *Iqbal*. *Arista II* essentially avoided any discussion of whether it was plausible to infer that the ISP subscriber was an infringer; therefore, it avoided noticing the concerns in unmasking motions

205. *See e.g. Sony Music*, 326 F. Supp. 2d at 567 (rejecting personal jurisdiction arguments as premature).

206. *See e.g. id.* at 567–568 (delaying the issue of personal jurisdiction).

207. *Id.* Personal jurisdiction involves determining whether a defendant has the necessary "minimum contacts" with the forum state. *Int'l Shoe*, 326 U.S. at 316.

208. *Sony Music*, 325 F. Supp. 2d at 567. The court relied primarily on the plaintiff's declaration. *Id.*

209. *See e.g. London-Sire*, 542 F. Supp. 2d at 180–181 (denying a motion to quash for lack of personal jurisdiction).

210. *See Carib. Broad. Sys., Ltd. v. Cable & Wireless PLC*, 148 F.3d 1080, 1090 (D.C. Cir. 1998) (finding that in the D.C. Circuit, where jurisdictional discovery is broadly granted, a good-faith belief that the court has jurisdiction is still necessary). Additionally, many of the First Amendment tests—including *Sony Music*—require a lack of non-privileged sources. *See e.g. Sony Music*, 326 F. Supp. 2d at 566 (requiring the plaintiffs to show that they have no other means to acquire the information).

that were similar to the concerns in *Twombly* and *Iqbal*. File-sharing subpoenas invade the privacy of privileged individuals and impose extensive discovery on third parties, concerns that were prominent in *Twombly* and *Iqbal*. Under the logic in those cases and the First Amendment concerns raised in *Mobilisa*, the defendant must be identified more specifically to avoid intrusive discovery and the identification of anonymous speakers not engaged in file-sharing. Thus, the *Sony Music* test should require allegations showing that the discovery sought can plausibly identify a specific defendant.

The Second Circuit's first error in *Arista II* was its refusal to reinterpret *Twombly* in light of the decision in *Iqbal*. In *Iqbal*, the U.S. Supreme Court addressed the Second Circuit's holding that claims must be amplified with factual allegations only when "such amplification is needed to render the claim plausible."[211] While the U.S. Supreme Court did not explicitly reject this language, it found that Iqbal's complaint was insufficient and reemphasized that *Twombly* applied to "all civil actions" including discrimination suits.[212] The Court also clarified that the plausibility analysis was fatal in *Twombly* because the analysis ignored conclusory allegations, and the Court proceeded to expand on what allegations could be considered conclusory.[213] In addition, the Court reemphasized that it did not discount Iqbal's claim because it was "unrealistic or nonsensical," but because it was conclusory.[214] This seems to be a repudiation of the Second Circuit's contextual application of the plausibility standard, yet the Second Circuit continued to apply this standard in *Arista II* and considered allegations based solely on information and belief.[215]

This contextual application of the plausibility standard leads the court to avoid the necessary plausibility question: whether it is plausible to infer that the subscriber is the one responsible for the infringement. The only allegation suggesting that a sub-

211. *Iqbal*, 129 S. Ct. at 1944 (emphasis removed). That holding, as recounted by the U.S. Supreme Court, seems to be that the factual matter required by *Twombly* was only needed in certain types of cases. *Id.*

212. *Id.* at 1951, 1953.

213. *Id.* at 1950; *id.* at 1960 (Souter, J., dissenting).

214. *Id.* at 1951 (majority).

215. *Arista II*, 604 F.3d at 120, 121 (quoting *Turkmen v. Ashcroft*, 589 F.3d 542, 546 (2d Cir. 2009)). The quoted standard, nearly identical to the one considered by the U.S. Supreme Court in *Iqbal*, merely quotes a case decided before *Iqbal*. *Id.*

scriber is the proper defendant is that his or her Internet connection was used in the infringement.[216] While *Iqbal* acknowledged that the court may make inferences, *Iqbal* made inferences with respect to *plausibility*, not with respect to what allegations are conclusory.[217] By merely inferring that there were no conclusory allegations, the court reduced this analysis to the holding that there was sufficient "factual detail."[218] The Court avoided explaining how and if that detail gives rise to the inference of liability. Instead, the Court merely refused to call the complaint insufficient because it did not see any way for the plaintiff to give more specific allegations.[219]

Thus, the *Arista II* court's motion-to-dismiss test promoted everything *Iqbal* and *Twombly* sought to avoid—allowing expensive discovery, giving meritless cases settlement value, and allowing invasive discovery of privileged defendants. While on an individual level, discovery of a handful of IP addresses may not be as large-scale as the antitrust discovery in *Twombly*, recent file-sharing cases list thousands of defendants.[220] Especially if this model grows, it would strain ISPs, which would be required to respond to the subpoenas, and individuals, who would have to comply with invasive discovery of their personal computers.[221] Further, the cost of defending and the desire to preserve anonymity create excessive incentive to settle, even in a case a defendant could win.[222] Just as the defendants in *Iqbal* had a qualified privilege,[223] anonymous defendants have First Amendment rights and privacy rights. Allowing discovery indiscriminately would both subject the innocent to the expense and inconvenience of discovery and invade the rights of Internet users by allowing discovery on the pretext of copyright infringement. One attorney noted how

216. *See* Compl., *Arista II*, *supra* n. 133, at 4 (explaining that the plaintiff only knew the defendants by their IP addresses or by their ISPs at the time of the infringement).

217. *Iqbal*, 129 S. Ct. at 1951–1952.

218. *Arista II*, 604 F.3d at 122. The court could be relying on the quotes from *Grokster* and *Aimster* indicating the popularity of file-sharing, but that seems to run directly counter to *Iqbal*'s description of the definition of "conclusory." *See Iqbal*, 129 S. Ct. at 1951 (rejecting that allegations are conclusory because they are "unrealistic or nonsensical").

219. *Arista II*, 604 F.3d at 122. Of course, the same could be said for the allegations in *Iqbal*.

220. *See* Anderson, *supra* n. 70 (reporting on a case with 23,322 defendants).

221. *See* Anderson, *supra* n. 71 (discussing the strain on ISP Time Warner Cable).

222. *Supra* nn. 189–194 and accompanying text.

223. *Iqbal*, 129 S. Ct. at 1953.

he could react to a defendant claiming someone else had been the downloader:

> **Option A:** We engage in discovery, seize all of the computers in the house, issue subpoenas to everyone the account holder knows, and start having depositions of everyone who lives in [the defendant's] home and neighborhood. By the time [we are] done, we not only will likely have gotten to the bottom of things, we would have flipped the defendant's entire life upside down. While that might get us somewhere, I prefer not to be that heavy-handed if I can avoid it.[224]

This type of discovery seems like exactly the sort of "fishing expedition" *Twombly* and *Iqbal* aimed to avoid.[225]

Rather, *Arista* should have considered whether the nonconclusory allegations gave rise to a plausible inference that the Doe subscriber was an infringer. This determination would require the plaintiff to consider and plead his or her methods of gathering information and identifying defendants.[226] This information would allow the court to make an explicit determination of whether the identification was specific enough to justify discovery. The court would be informed of how the IP addresses are generated and turned into names, and how accurate the process is at each step. This determination would not necessarily bar all John Doe actions—it would simply require more allegations that identify the infringer and link him or her to the investigation results that turned up the IP address.

This requirement minimizes suits that would chill speech and avoids conducting extensive discovery just to identify the defendant. By insisting on a specific link between the IP address and the infringer, courts can eliminate claims that are merely based on a pretext of copyright infringement. Similarly, claims based on

---

224. Marc Randazza, TorrentFreak, *Are You Guilty if Pirates Use Your Internet? Lawyer Says Yes*, http://torrentfreak.com/are-you-guilty-if-pirates-use-your-internet-lawyer-says-yes-110806/ (Aug. 6, 2011). "Option B" is to use a negligence claim, which would hold the defendant liable for letting others use his or her Internet connection, to pressure the defendant into settling. *Id.*

225. *See* Clermont, *supra* n. 156, at 850 (noting that *Twombly* aims to avoid so-called "fishing expeditions").

226. *See* Piatek et al., *supra* n. 68, at 2 (comparing "direct detection" with "indirect detection" and noting that while direct detection is more accurate, some investigators use indirect detection instead when monitoring BitTorrent).

mistaken downloads can also be weeded out with more information concerning the plaintiffs' investigations. Minimizing these two sources of non-infringing defendants keeps claims from chilling protected speech and legal file-sharing. Additionally, requiring a specific link reduces the need for extensive discovery to determine who the defendant is—or at least ensures that discovery has a focused scope. It also forces plaintiffs to make real efforts to distinguish between the actual infringer and the easy target of the Internet subscriber; thus, this requirement would satisfy both *Mobilisa*'s First Amendment concerns as well as *Iqbal*- and *Twombly*-related policy concerns.

### D. Denouement: What Happens to Plaintiffs?

In light of criticisms of *Iqbal*, many would respond to this standard with concern for the plaintiff, but their worry would be misplaced because copyright owners were never well served by John Doe suits to begin with. The RIAA litigation campaign did not seem to make money,[227] and its success in deterring piracy is dubious,[228] leading the group to call off its campaign.[229] More recent attempts at profiting from these suits rely on massive misjoinder, lack of personal jurisdiction, and quick out-of-court settlements, which have already angered some judges.[230] If these suits have been profitable at all, it is only because they have been avoiding actual court proceedings aside from the initial unmasking.[231] This procedure can hardly be called useful, and the need to stop piracy can no longer justify the procedure given such lackluster success.

227. Fogarty, *supra* n. 16, at 150.

228. *Compare id.* (claiming the illegality of file-sharing has been "learned and ignored" by the public) *with* Recording Indus. Ass'n of Am., *supra* n. 58 (suggesting the litigation campaign curbed piracy rates).

229. Recording Indus. Ass'n of Am., *supra* n. 58.

230. Anderson, *supra* n. 70 (reporting on a judge requiring plaintiffs to show cause why parties were joined and under the personal jurisdiction of the court); Samuels, *supra* n. 9 (quoting several rulings hostile to "copyright trolls").

231. *See* Samuels, *supra* n. 9 (explaining that plaintiffs appear to be using the courts to reveal the identities of possible defendants so they can obtain a settlement outside of court).

## *VI. CONCLUSION*

Ultimately, the drawbacks of John Doe suits make them more of a stopgap than a permanent solution for the tension between file-sharers and copyright laws. For a more permanent solution, however, copyright owners and legislators should look to other sources. As *Sony* noted, where new technology is concerned, Congress is better suited than the courts to weigh all the competing interests.[232] Several legislative solutions have already been proposed, including an alternative dispute resolution system or a system of levies.[233] Alternate business models for record labels have also been proposed to make them less dependent on record sales.[234] In the long run, the John Doe suit should be phased out in favor of better enforcement opportunities, alternative business methods, and long-term solutions to piracy. Limiting John Doe suits may speed along this process, but more importantly, it will help calm public fears of reckless accusations and force copyright owners to be accountable for their actions in court when unmasking possible defendants.

232. *Sony*, 464 U.S. at 456.

233. *See generally* Lemley & Reese, *supra* n. 27, at 1406–1424 (describing a proposed system of levies and a streamlined dispute resolution system). Any dispute resolution would be subject to the First Amendment, but it could be structured to better maintain anonymity and privacy. Legislative solutions must also carefully balance freedom of speech issues and privacy issues, but recent events have shown that the public is willing to pressure Congress over these issues. *See* Timothy B. Lee, *Ars Technica*, *Tech Policy*, *News*, *Under Voter Pressure, Members of Congress Backpedal (Hard) on SOPA*, http://arstechnica.com/tech-policy/news/2012/01/under-voter-pressure-members-of-congress-backpedal-on-sopa.ars (Jan. 14, 2012, 11:55 a.m.) (reporting on how members of Congress and the Obama administration withdrew their support for the Stop Online Piracy Act after Internet protests concerning the bill's effects on freedom of speech and other issues); *see also* Eric Goldman, *Ars Technica*, *Tech Policy*, *News*, *The OPEN Act: Significantly Flawed, but More Salvageable than SOPA/PROTECT-IP*, http://arstechnica.com/tech-policy/news/2011/12/the-open-act-significantly-flawed-but-more-salvageable-than-sopaprotect-ip.ars (Dec. 12, 2011, 7:40 a.m.) (analyzing OPEN, an alternative to SOPA also seeking to address Internet piracy).

234. *See generally* Fogarty, *supra* n. 16, at 170–174 (proposing alternative business models for record labels).