Vanderbilt Journal of Entertainment & Technology Law

Volume 22
Issue 1 *Issue 1 - 2019*

Article 5

2019

Weeding out Wolves: Protecting Speakers and Punishing Pirates in Unmasking Analyses

Nathaniel Plemmons

Weeding Out Wolves: Protecting Speakers and Punishing Pirates in Unmasking Analyses

ABSTRACT

How should courts determine whether to expose an anonymous internet speaker's identity? Millions of Americans anonymously use the internet. The overwhelming majority of anonymous users obscure their identity while engaging in political or otherwise protected speech. A substantial minority, however, obfuscate their true identity while defaming others, pirating intellectual property, and otherwise breaking the law to escape liability for their wrongful actions, crying "free speech" when sued. Courts tread a razor-thin line between protecting legitimate exercises of free speech and exposing wrongdoers, as wrongful disclosure chills speech and exposes innocent persons to the very real threat of doxing. Conversely, failure to grant discovery into IP theft in a timely manner imposes significant penalties on the injured party and the economy at large given the huge sums of money bled out over time and practical difficulties associated with actually unmasking bad actors. Currently, courts trend between two tests that overprotect bad acts while underprotecting legitimate speech. Courts should instead adopt a defendant-friendly standard with a presumption in favor of unmasking defendants in IP piracy cases so as to protect legitimate speech while providing a shortcut to unmask wolves in free-speech clothing.

TABLE OF CONTENTS

"While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace—the 'vast democratic forums of the Internet' in general and social media in particular."[1] Justice Kennedy's assertion in *Packingham v. North Carolina* is well supported. According to the latest Pew studies, over 89 percent of US adults used the internet in 2018, a rate that cut across virtually every demographic.[2] Social media holds a central position in modern discourse, as millions of Americans utilize Facebook, Instagram, Twitter, and other platforms each day.[3] Through status updates, tweets, and direct messages, approximately seven out of ten Americans shared and exposed themselves to many different ideas over social media in 2018.[4] Indeed, over 60 percent of Facebook, Snapchat, and Instagram account holders use these sites daily.[5] Additionally, over 80 percent of Americans own a smartphone—devices capable of (and principally designed for) accessing the internet and social media on the go.[6] The development of smartphones not only increased internet and

1. Packingham v. North Carolina, 137 S. Ct. 1730, 1735 (2017).

2. *Internet/Broadband Fact Sheet*, PEW RES. CTR.: INTERNET & TECH. (June 12, 2019), http://www.pewinternet.org/fact-sheet/internet-broadband/ [https://perma.cc/HTN3-TGR2].

3. *Social Media Fact Sheet*, PEW RES. CTR.: INTERNET & TECH. (June 12, 2019), http://www.pewinternet.org/fact-sheet/social-media/ [https://perma.cc/99KM-UP2E].

4. *Id.*

5. *Id.*

6. *Mobile Fact Sheet*, PEW RES. CTR.: INTERNET & TECH. (June 12, 2019), http://www.pewinternet.org/fact-sheet/mobile/ [https://perma.cc/QP62-WCL].

social media use; it allowed individuals to communicate in real time simply by removing a cellphone from their back pocket.

As the prominence of internet speech increases, so too does the ease of speaking anonymously. Most social media websites do not require profiles to be linked to a person's real-world identity.[7] This anonymity presents a free-speech problem for courts in a variety of legal disputes involving the internet. Hypotheticals A, B, and C below demonstrate some ways this problem manifests itself.

In hypothetical A, Adrienne works as Andrew's secretary. Andrew is a bad boss, micromanaging Adrienne and her peers while at the same time disappearing whenever he is actually needed. Adrienne wants to warn others not to come work for her office without getting reprimanded, fired, or otherwise punished for speaking poorly (though truthfully) of her employer. Her solution: create an anonymous account on Glassdoor and leave a scathing—but true—review of Andrew. Andrew finds this review, becomes infuriated, and wants to sue whoever left it for defamation to silence their (legitimate) criticism.[8]

In hypothetical B, Betsy works as Bryan's secretary. Betsy treats customers with disdain, poorly maintains Bryan's schedule, and consistently shows up to work late. Bryan, upset with Betsy's performance and attitude, decides to fire her. Angered, Betsy wants revenge. However, she does not want Bryan to trace her actions back to her. Her solution: create an anonymous account on Glassdoor and leave a scathing (and *untrue*) review of Bryan. Bryan is aghast when he finds this review. Despite being untrue, the review may damage his reputation and business. Bryan wants to sue the anonymous speaker who left the review for defamation.[9]

In hypothetical C, Chris, the owner of a local café, designed and registered a prototype coffee bean grinder that could be made using a 3D printer. One day, while browsing a 3D printer file marketplace,[10] Chris saw that an anonymous user posted a coffee bean grinder file with his exact design. Infuriated, Chris wants to sue the user that stole and posted his design.

---

7. *See* discussion *infra* Section I.E.

8. See *infra* Section II.D.2 for a case that mirrors these facts, Glassdoor, Inc. v. Andra Grp., LP, 560 S.W.3d 281 (Tex. App. 2017), *vacated*, 575 S.W.3d 523 (Tex. 2019) (finding that the underlying cause of action was moot).

9. See *infra* Section II.D.1 for a case that mirrors these facts, *In re* Elliott, 504 S.W.3d 455 (Tex. App. 2016).

10. For example, 3dprintboard.com is a forum where users can discuss and trade files for 3D printing. 3DPRINTBOARD.COM, https://3dprintboard.com/ [https://perma.cc/4H76-N9MJ] (last visited Sept. 12, 2019).

All three plaintiffs file hypothetical complaints in the same district court, seeking to uncover who left the damaging reviews or infringed on their design. How should courts balance the need to vindicate an injured plaintiff's rights with that of protecting an anonymous internet speaker's First Amendment rights?[11] Should it differentiate between claims of defamation and infringement? Moreover, even if it allows discovery, how is an anonymous internet speaker actually located and unmasked?

This Note examines the prevalence of anonymous internet speakers, the practical and legal issues that courts confront when balancing the rights of anonymous internet speakers with those of plaintiffs seeking to unmask them, and the serious dangers courts expose speakers to if wrongfully unmasked. Part I argues that internet speech merits the same First Amendment protections as traditional speech, notes the unique benefits of anonymous internet speech, examines the practical difficulties faced by courts and plaintiffs in unmasking anonymous speakers, and details the immense dangers these speakers face if wrongfully exposed. Part II analyzes the most common approaches courts use when determining whether to unmask an anonymous internet speaker, argues for the special treatment of intellectual property claims within unmasking analyses, and grounds the discussion by walking the reader through cases highlighting the recent internet free-speech controversy in Texas. Finally, Part III argues that, because the vast majority of courts treat internet and traditional speech interchangeably and favor protecting anonymous speech, anonymous internet speakers' identity should be protected under a defendant-friendly standard with a rebuttable presumption in favor of the plaintiff in IP infringement cases.

I. BACKGROUND

A. The First Amendment Offers Broad, but not Unlimited, Protection of Speech

The Supreme Court has long recognized that the First Amendment offers broad, but not unconditional, protection to various types of speech based on content. For example, obscene speech, true threats, and fighting words are unprotected by the First Amendment, and restrictions on such speech need only pass rational basis review.[12]

---

11. A discussion of why a First Amendment protects a right to anonymous free speech on the internet can be found below. *See infra* Sections II.B–C.

12. *See* Virginia v. Black, 538 U.S. 343, 359 (2003) (holding that the First Amendment permits a state to ban true threats); Sable Commc'ns of Cal., Inc. v. FCC, 492 U.S. 115, 124 (1989)

In contrast, political and controversial speech receive the highest possible First Amendment protection under strict scrutiny review.[13] Separate still are other kinds of speech, like commercial speech, receiving intermediate scrutiny review.[14] This Note addresses anonymous internet speech, a categorization concerned with the speech's form rather than its content. The Supreme Court firmly rejected the idea that internet speech should be deprived of First Amendment protections merely because it takes place online.[15]

B. The First Amendment Protects a Right to Anonymous Free Speech

The US Supreme Court has repeatedly held that the First Amendment protects the right to speak anonymously.[16] For example, in *McIntyre v. Ohio Elections Commission*, the Supreme Court confronted a statute that prohibited the dissemination of campaign literature that did not list the name or address of the person issuing it.[17] Writing for the majority, Justice Stevens concluded:

> [U]nder our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from

---

(noting that the Court has "repeatedly held that the protection of the First Amendment does not extend to obscene speech"); Cohen v. California, 403 U.S. 15, 20 (1971) (holding that fighting words are not protected under the First Amendment).

13. *See* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 340 (2010) (quoting Fed. Election Comm'n v. Wis. Right to Life, Inc., 551 U.S. 449, 464 (2007) (opinion of Roberts, C.J.)) ("Laws that burden political speech are 'subject to strict scrutiny,' which requires the Government to prove that the restriction 'furthers a compelling interest and is narrowly tailored to achieve that interest.'"); R.A.V. v. City of St. Paul, Minn., 505 U.S. 377, 391 (1992) (holding that "[t]he First Amendment does not permit [the imposition of] special prohibitions on those speakers who express views on disfavored subjects," even expressive acts as extreme as cross burning, under strict scrutiny).

14. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 562–63 (1980) (citing Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456–57 (1978)) ("The Constitution therefore accords a lesser protection to commercial speech than to other constitutionally guaranteed expression.").

15. *See* discussion *infra* Section I.C.

16. *See, e.g.*, Buckley v. Am. Constitutional Law Found., Inc., 525 U.S. 182, 199–200, (1999); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995); Talley v. California, 362 U.S. 60, 60–61, 65 (1960) (invalidating a statute that prohibited distribution of handbills without the name and address of the preparer); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462–63 (1958) (compulsory disclosure of names of individuals engaging in activity protected under the First Amendment right to freedom of association impermissibly created a "likelihood of a substantial restraint" upon the exercise of protected activity that could result in a "repressive effect").

17. *McIntyre*, 514 U.S. at 357.

> retaliation—and their ideas from suppression—at the hand of an intolerant society.[18]

The Court reached a similar conclusion in *Buckley v. American Constitutional Law Foundation*.[19] In *Buckley*, the Court confronted a state statute that forced petition circulators to wear identification badges.[20] To qualify for these badges, prospective circulators had to submit their names, addresses, and the amount of money they received for circulating petitions.[21] The Court found that this requirement impermissibly burdened the circulator's First Amendment rights because it "compel[led] . . . identification at the precise moment when the [speaker]'s interest in anonymity [was] greatest."[22]

In the United States, anonymous speech has a long and cherished history, playing an invaluable societal role from the nation's founding through modernity. As Justice Black noted, "Anonymous [speech has] played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all."[23] Some of the most iconic US works were published anonymously or pseudonymously in fear of retribution. As Justice Black noted, "[T]he Federalist Papers, written in favor of the adoption of our Constitution . . . [were] published under fictitious names."[24] Indeed, Justice Stevens devoted an entire footnote in *McIntyre* to the value of anonymous speech, noting that figures from Mark Twain and Ben Franklin to Voltaire and Shakespeare all employed pseudonyms to protect their identity.[25] He also noted that many anonymous speakers have myriad legitimate reasons for choosing to conceal their identity, stating that "[t]he decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible."[26] Thus, the *McIntyre* Court held that the First Amendment protects a speaker's "decision to remain anonymous."[27]

---

18. *Id.* (citations omitted).
19. *Buckley*, 525 U.S. at 199–200.
20. *Id.* at 188–89.
21. *Id.*
22. *Id.* at 199; *see also* Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 166–67 (2002) (holding that requiring a religious canvasser to register their name in a publicly available document implicated the canvasser's anonymity interests and violated their First Amendment rights).
23. Talley v. California, , 362 U.S. 60, 64 (1960).
24. *Id.* at 65.
25. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341 n.4 (1995).
26. *Id.* at 341–42.
27. *Id.* at 342.

C. Internet Speech Merits the Same Protections and Limitations as Traditional Speech

Justice Stevens's statement that "the freedom to publish anonymously extends beyond the literary realm" has far-reaching implications.[28] In *Reno v. ACLU*, the Court addressed the applicability of First Amendment protections to online communications.[29] Overturning an overly vague state statute regulating the content of online discussion, the Court explicitly characterized internet speech in the same terms as traditional speech: "Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer."[30] After finding that the Court's "cases provide *no basis* for qualifying the level of First Amendment scrutiny that should be applied to [the internet]," it invalidated the statute under strict scrutiny.[31]

In *Ashcroft v. American Civil Liberties Union*, the Court once again applied a First Amendment strict scrutiny test when it upheld a preliminary injunction concerning the Child Online Protection Act (COPA).[32] Staying true to the principle put forth in *Reno*, the fact that the speech took place on the internet had no bearing on the level of First Amendment scrutiny the Court applied when it delivered its judgment.[33]

In 2017, the Court went further in exploring the connection between internet and traditional speech in a case where North Carolina passed a statute foreclosing social media access to sex offenders altogether.[34] "While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. *It is cyberspace*—the 'vast democratic forums of the Internet' in general and social media in

---

28. *Id.*

29. Reno v. ACLU, 521 U.S. 844 (1997).

30. *Id.* at 870, 885; *see also* Best W. Int'l, Inc. v. Doe, No. CV–06–1537–PHX–DGC, 2006 WL 2091695, at *3 (D. Ariz. July 25, 2006) (citing *Reno*, 521 U.S. at 870); Sony Music Entm't Inc. v. Does 1–40, 326 F. Supp. 2d 556, 562 (S.D.N.Y. 2004) (citing *Reno*, 521 U.S. at 870; Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001); Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999)) ("Courts have recognized the Internet as a valuable forum for robust exchange and debate.").

31. *Reno*, 521 U.S. at 870, 874 (emphasis added).

32. Ashcroft v. ACLU, 542 U.S. 656, 673 (2004).

33. *Id.* at 658; *Reno*, 521 U.S. at 870.

34. Packingham v. North Carolina, 137 S. Ct. 1730 (2017).

particular."[35] The Court explained that internet speech merits treatment equal to traditional speech given the internet's central place in modern discourse.[36] Indeed, the Court held that "to foreclose access to social media altogether is to prevent the user from engaging in the legitimate exercise of First Amendment rights."[37]

If internet speech is equal to traditional speech, it should receive the same level of protection.[38] The Court applied this principle in *Reno* when it held that its "cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium [i.e., the internet]."[39] According to the Court, the "content found on the Internet is as diverse as [the range of] human thought" and as such should not be unduly constrained.[40] This equal treatment comports with the Court's decisions in *Reno, Ashcroft,* and *Packingham.*[41] Moreover, as the equal of traditional speech, it follows that "the protection of Internet speech also includes the protection of anonymous electronic speech."[42] Thus, courts should analyze both internet and traditional speech under the same levels of scrutiny based on the speech's content regardless of the medium through which the speaker communicates.[43]

D. Anonymous Speech Is Particularly Prevalent and Valuable in the Internet Context

The internet is particularly conducive to anonymous speech. Indeed, many websites operate on the assumption that users have a right to speak anonymously. For example, Reddit, Twitter, and WordPress are often used by anonymous speakers to express themselves. Sexual and domestic abuse survivors, corporate whistleblowers, and controversial political activists all use these and other platforms to maintain their anonymity. These and other similarly sensitive topics benefit from—or in many cases, require—the ability for speakers to maintain their anonymity. On Reddit, in particular, countless people communicate and seek support anonymously

35. *Id.* at 1735 (emphasis added) (citation omitted).

36. *Id.*

37. *Id.* at 1737.

38. *See Reno*, 521 U.S. at 870.

39. *See id.*

40. *Id.* at 852 (quoting ACLU v. Reno, 929 F. Supp. 824, 842 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997)).

41. *See Packingham*, 137 S. Ct. at 1735; Ashcroft v. ACLU, 542 U.S. 656, 673 (2004); *Reno*, 521 U.S. at 870.

42. *In re* Does 1–10, 242 S.W.3d 805, 820 (Tex. App. 2007) (citing Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001)).

43. *See Packingham*, 137 S. Ct. at 1735; *Ashcroft*, 542 U.S. at 673; *Reno*, 521 U.S. at 870.

concerning sensitive topics that they feel unable to discuss under their real names on "subreddits," such as r/relationships, r/divorce, r/confessions, r/TwoXChromosomes, and r/anxiety, to name just a few.[44] Many of these subreddits have hundreds of thousands, if not millions, of anonymous posters and readers.[45]

Justice Stevens, however, noted that many persons speak anonymously or pseudonymously because they fear unjust repercussions for exercising their right to free speech.[46] In particular, the phenomenon of strategic lawsuits against public participation (SLAPPs) loom large in the modern anonymous speaker's mind.[47] SLAPPs are retaliatory suits brought by parties to intimidate and silence those who have spoken out in the public sphere.[48] The actual resolution of the plaintiff's claims is largely secondary to their ultimate goal of dissuading the defendant from engaging in damaging, offending, or otherwise undesirable speech through drawn out, costly litigation.[49] While anti-SLAPP statutes often help such defendants quickly shut down these suits, many try to sidestep the problem altogether by speaking anonymously.[50] For example, Adrienne in hypothetical A posted anonymously because she (correctly) feared that Andrew would attempt to sue her for exercising her right to speak truthfully.

Anonymous internet speakers also provide unique value in the form of anonymous ratings and reviews. For example, users on Glassdoor can post in a "Company Reviews" section, rating and leaving reviews of their experiences as employees for a given business, which allows prospective employees to "[g]et the inside scoop and find out what it's really like from people who've actually worked there." [51] This feature provides insight into aspects of the employer's culture that may

---

44. Subreddits are subcommunities on the website Reddit.com devoted to certain topics denoted by their names. *See infra* note 45.

45. *See, e.g.*, *r/Anxiety*, REDDIT, https://www.reddit.com/r/anxiety [https://perma.cc/5A6Y-3PZZ] (last visited Sept. 12, 2019) (286,000 readers); *r/relationships*, REDDIT, https://www.reddit.com/r/relationships/ [https://perma.cc/EAR8-22UD] (last visited Sept. 12, 2019) (2.6 million readers); *r/TwoXChromosomes*, REDDIT, https://www.reddit.com/r/TwoXChromosomes/ [https://perma.cc/3TVF-8ARH] (last visited Sept. 12, 2019) (12.5 million readers).

46. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341–42 (1995).

47. *Anti-SLAPP Statutes and Commentary*, MEDIA L. RESOURCE CTR., https://www.medialaw.org/topics-page/anti-slapp?tmpl=component&print=1 [https://perma.cc/6MFD-RUX4] (last visited Sept. 6, 2019).

48. *Id.*

49. *Id.*

50. *Id.*

51. *See Company Reviews*, GLASSDOOR, https://www.glassdoor.com/Reviews/index.htm [https://perma.cc/C27U-KPEG] (last visited Sept. 12, 2019).

not be readily apparent during the application process.[52] Similarly, Yelp allows users to anonymously review their experiences with businesses and service providers—ranging from dentists to restaurants to mechanics—to help other Yelp users make choices on those vendors in the future.[53] The ability to speak anonymously can be critical to users sharing information freely.

Courts value anonymous internet speech. Confronted with a case in which the plaintiffs sought to unmask anonymous individuals for online defamatory comments, the US District Court for the Western District of Washington noted:

> The free exchange of ideas on the Internet is driven in large part by the ability of Internet users to communicate anonymously. If Internet users could be stripped of that anonymity by a civil subpoena enforced under the liberal rules of civil discovery, this would have a *significant* chilling effect on Internet communications and thus on basic First Amendment rights.[54]

In *Columbia Insurance Company v. Seescandy.com*, the Northern District of California held that the rights of injured parties must be

> balanced against the legitimate and valuable right to participate in online forums anonymously or pseudonymously . . . Th[e] ability to speak one's mind without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate. Furthermore, it permits persons to obtain information relevant to a sensitive or intimate condition without fear of embarrassment. People who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity.[55]

Several other courts that confronted plaintiffs trying to unmask anonymous defendants made similar remarks concerning balancing a plaintiff's right to redress their grievances with a defendant's right to anonymous speech.[56] Given the unique First Amendment value of anonymous internet speech, it is unsurprising that courts show reluctance in granting motions seeking to unmask anonymous individuals online.

---

52. *Id.*

53. *See* YELP, https://www.yelp.com [https://perma.cc/8V79-THPK] (last visited Jan 18, 2020).

54. Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001) (emphasis added).

55. Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999).

56. *See, e.g.*, Sony Music Entm't Inc. v. Does 1–40, 326 F. Supp. 2d 556, 562 (S.D.N.Y. 2004) ("Courts have recognized the Internet as a valuable forum for robust exchange and debate.") (citations omitted); *In re* Does 1–10, 242 S.W.3d 805, 820 (Tex. App. 2007) ("Several courts have noted that Internet anonymity serves a particularly vital role in the exchange of ideas and robust debate on matters of public concern.") (citations omitted).

E. Anonymous Internet Speech Presents Unique Problems to Courts

The First Amendment does not unconditionally protect all forms of speech and expression, regardless of whether the speech is traditional or digital.[57] Individuals can create and be liable for online personas tied to their real-life identities. For example, the Court in *Elonis v. United States* evaluated the conviction of a defendant under 18 U.S.C. § 875(c), which criminalizes the interstate transmission of threats to another person.[58] Elonis posted numerous Facebook status updates containing self-styled rap lyrics concerning his estranged wife, police officers, a kindergarten class, and an FBI agent.[59] These lyrics were staggeringly violent, describing the ways he would kill each of the concerned parties in graphic detail.[60] The Court assumed the statute was a constitutional regulation of internet speech but reversed Elonis's conviction on statutory grounds.[61]

Anonymous internet speech, however, presents unique problems to courts. Though "anonymous [speakers] . . . have a First Amendment right to anonymous speech on the Internet, that right is subject to limitation" in the same way as traditional speech.[62] As a Virginia Circuit Court of Appeals noted, "Those who suffer damages as a result of tortious or other actionable communications on the Internet should be able to seek appropriate redress by preventing the wrongdoers from hiding behind an illusory shield of purported First Amendment rights."[63] Anonymous users can, and often do, attempt to escape liability for defamation and infringement actions, among others, by hiding behind a false persona and crying "free speech" when sued.[64] This is exactly what Betsy and the anonymous user in hypotheticals B and C did when they defamed Bryan and infringed on Chris's design, respectively.

It is difficult to understate the lengths that courts and counsel undergo to unmask anonymous individuals that abuse their First

---

57. *See supra* Sections II.B–C.

58. Elonis v. United States, 135 S. Ct. 2001, 2007 (2015).

59. *See id.*

60. *See id.* at 2005–07.

61. *See id.* at 2011.

62. *In re* Does 1–10, 242 S.W.3d 805, 820 (Tex. App. 2007) (citing Polito v. AOL Time Warner, Inc., 78 Pa. D. & C.4th 328 (Ct. Com. Pl. 2004)); *see also* Ashcroft v. ACLU, 542 U.S. 656, 673 (2004) (applying strict scrutiny to a First Amendment challenge to a restriction on internet speech); Reno v. ACLU, 521 U.S. 844, 870 (1997) (applying the same).

63. *In re* Subpoena Duces Tecum to Am. Online, Inc., 52 Va. Cir. 26, 35 (2000), *rev'd sub nom on other grounds*, Am. Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377 (Va. 2001).

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

Amendment rights. Anonymous users can sign up for a myriad of websites, provide an email, chose a pseudonym, and become a posting member in less than a minute.[65] One need not provide a legitimate email connected to their actual identity. Instead, internet users can connect a fake email to a fake account on a website or social media.[66] One can even mask their IP address with the use of a virtual private network (VPN) as they browse and post on the internet. One of the most prominent VPNs is The Onion Router (TOR). By utilizing TOR, users can bounce their IP address across several different servers, burying the connection between their activities and the computer they used beneath layers of encryption and misdirection.[67] Though TOR and its advocates assert that its primary purpose is to ensure privacy (if not the ability to circumvent highly repressive regimes[68]), there are abundant examples of its abuse.[69] This leaves plaintiffs like Bryan and Chris in a difficult position; even if the court grants discovery, there is no guarantee that it will successfully reveal the user's identity.

There are new tools, however, that may allow courts and counsel to expose defendants hiding behind multiple masks. For example, one professor claims that he has developed a way to piece TOR's layers back

---

65. For example, one can create a Twitter account by providing a username (by no means one's real name) and email. So long as the username has yet to be taken, the account opens immediately. *Sign Up*, TWITTER, https://twitter.com/i/flow/signup [https://perma.cc/QT3J-XXT5] (last visited Sept. 12, 2019).

66. For example, one can create a Gmail account by providing a name and date of birth (again, by no means one's real name or date of birth). So long as the name is unique, the account opens immediately. *Sign Up*, GOOGLE, https://accounts.google.com/signup [https://perma.cc/ZC5M-NZ6T] (last visited Sept. 12, 2019).

67. *See Tor: Overview*, TOR, https://www.torproject.org/about/overview.html [https://perma.cc/8PAR-66PE] (last visited Sept. 12, 2019).

68. For example, countries such as Burkina Faso and Uzbekistan show some of the highest TOR usage rates, allowing "people in those circumstances to do things that they otherwise would not be able to do." *See* Joseph Cox, *Countries That Use Tor Most Are Either Highly Repressive or Highly Liberal*, MOTHERBOARD (Apr. 6, 2016, 9:40 AM), https://motherboard.vice.com/en_us/article/8q8xga/countries-that-use-tor-most-are-either-highly-repressive-or-highly-liberal [https://perma.cc/7CGS-5MCH].

69. One incredibly relevant example is the rise and fall of the first Silk Road website on TOR, where individuals shrouded behind several layers of anonymity purchased illicit drugs, fake IDs, and other commodities using cryptocurrency. *See* Marcell Nimfuehr, *Silk Road: A Cautionary Tale About Online Anonymity*, MEDIUM (Aug. 18, 2018), https://medium.com/s/story/the-silk-road-a-real-thriller-and-the-truth-about-the-anonymity-of-bitcoin-198b519ca397 [https://perma.cc/7V68-Y9TX]. Indeed, a recently created graphic shows over six thousand websites on TOR where individuals view, promote, and utilize "violence . . . racism . . . extreme sexual content, credit card cloning products . . . a large number of Bitcoin scams," and numerous other deeply concerning topics. Thomas Brewster, *This Insane Map Shows All the Beauty and Horror of the Dark Web*, FORBES (Mar. 13, 2018, 5:20 PM), https://www.forbes.com/sites/thomasbrewster/2018/03/13/dark-web-map-6000-webpages/#1e95867b648b [https://perma.cc/785F-MNQY].

together.[70] Boasting an 81 percent success rate in 2014, this tool could be the first of many that plaintiffs can use to unmask defamers and infringers hiding in the internet's dark corners.[71] However, annoyed parties like Andrew in hypothetical A can just as easily use this tool to "SLAPP" the very users that need online anonymity the most.[72]

But how do the benefits of unmasking these bad actors compare with the costs inflicted on those who need the protections of anonymous speech to participate in public discourse? Indeed, many internet users will not voice their political opinions without the protection of anonymity. Speakers fear that individuals with varying tolerance for "offensive" or "intolerant" speech will attempt to identify, persecute, and, in some cases, harm internet speakers who voice unpopular or contrarian views by "doxing" them.[73] For example, doxing is often the tactic most successfully (though by no means exclusively) utilized by "far-left internet extremists" like Antifa to inflict "social and economic punishment."[74] Despite the fact that their speech is protected under the First Amendment,[75] victims of doxing have been harassed by anonymous mobs, lost their jobs, and even been physically attacked for their exercise of speech.[76]

Illustrating its magnitude, a recent Department of Justice bulletin addressed doxing as a form of particularly dangerous cyber harassment, explaining that "[i]t can expose the victim to an anonymous mob of countless harassers, calling their phones, sending them email, and even appearing at the victim's home."[77] The bulletin gave the example of Zoe Quinn, a victim of doxing whose real name, home address, email, passwords, and family details were exposed.[78] Though Quinn was never physically confronted, she received thousands of threats—including threats of rape and death—as a result of being

---

70. Swati Khandelwal, *81% of Tor Users Can Be Easily Unmasked by Analysing Router Information*, HACKER NEWS (Nov. 18, 2014), https://thehackernews.com/2014/11/81-of-tor-users-can-be-easily-unmasked_18.html [https://perma.cc/86WD-E9S3].

71. *Id.*

72. *See* discussion *supra* Section I.D.

73. Doxing is an attempt by one party to uncover information leading to an online speaker's real-world identity for the sake of harassment. *See* Joey L. Blanch & Wesley L. Hsu, *An Introduction to Violent Crime on the Internet*, U.S. ATTORNEYS' BULL., May 2016, at 2, 5.

74. Emma Grey Ellis, *Whatever Your Side, Doxing Is a Perilous Form of Justice*, WIRED (Aug. 17, 2017, 8:00 AM), https://www.wired.com/story/doxing-charlottesville/ [https://perma.cc/N9MH-VW9B].

75. *See supra* Section I.A.

76. *See infra* notes 78–80, 231–33, and accompanying text.

77. *See* Blanch & Hsu, *supra* note 73, at 5.

78. *Id.* at 5–6.

doxed.[79] Another example is that of Fox News anchor Tucker Carlson. Tweets containing his personal information led to a group of Antifa members appearing outside his home in what is now being investigated as a politically motivated hate crime.[80]

It follows that there is a great need for courts to settle on a test for unmasking individuals that vindicates an injured plaintiff's right to expose wolves in free-speech clothing. At the same time, courts must protect an individual's right to speak anonymously on the internet with more than a paper tiger.[81]

F. Seescandy.com *as the First Prominent Unmasking Case*

One of the first cases that created a test for unmasking anonymous internet speakers was *Seescandy.com* in 1999. In that case, Columbia Insurance Company, the holding company of See's Candy, asked the Northern District of California to issue a temporary restraining order (TRO) against the owners of seescandy.com.[82] However, the anonymous defendant hid his email, physical address, phone number, and name of the domain owner behind layers of false information.[83] Columbia's attempts to identify him were unsurprisingly unsuccessful.[84] As such, the court denied Columbia's motion as futile because they could not gather the information required to serve the defendant within a TRO's highly limited timeframe.[85] Further, they could not obtain a preliminary injunction either, because courts cannot grant such relief ex parte.[86]

Ultimately, the court noted a limited exception to the rule that discovery can only commence after the defendant receives service, seeking to avoid the defendant's attempt to hide its identity.[87] The court

---

79. *Id.*

80. *See* Jessica Chasmar, *Fox News Boycotts Twitter Over Handling of Tucker Carlson Doxing: Reports*, WASH. TIMES (Nov. 12, 2018), https://www.washington-times.com/news/2018/nov/12/fox-news-boycotts-twitter-over-handling-tucker-car/ [https://perma.cc/A36F-KKCJ]. For an example of a group doxed for exercising their right to political speech, see discussion *infra* Part III.

81. Merriam-Webster defines paper tiger as the following: "One that is outwardly powerful or dangerous but inwardly weak or ineffectual." *Paper Tiger*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/paper%20tiger [https://perma.cc/VL8N-6G2W] (last visited Sept. 12, 2019).

82. Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 575 (N.D. Cal. 1999).

83. *Id.* at 577.

84. *Id.*

85. *Id.*

86. *Id.*

87. *Id.*

found that the exception applied in this case, given the way the internet gave individuals

> the ability to commit certain tortious acts, such as defamation, copyright infringement, and trademark infringement, entirely on-line . . . Parties who have been injured by these acts are likely to find themselves chasing the tortfeasor from Internet Service Provider (ISP) to ISP, with little or no hope of actually discovering the identity of the tortfeasor.[88]

Thus, the court denied Columbia's motion without prejudice and ordered it to refile within fourteen days, because it wanted Columbia to establish several factors prior to the court's grant of preservice discovery.[89] The court ordered the plaintiff to (1) identify the missing party with sufficient specificity so a court could determine that the defendant is a real person or entity who could be sued in federal court, (2) identify all previous steps taken to locate the defendant, (3) establish that the plaintiff's suit could withstand a motion to dismiss, and (4) file a statement of reasons justifying the specific discovery requested as well as some identification of a limited number of persons or entities on whom the discovery process might be served.[90] The court found that Columbia satisfied elements one through three and ordered it to return in fourteen days with a discovery request, statement of reasons, and identification of parties that would satisfy element four.[91] As detailed below, unmasking analyses would only expand from here.

II. ANALYSIS

Free-speech protections—including the right to speak anonymously—apply to expressive activity with as much force on the internet as they do in the public square.[92] Furthermore, threats to a speaker's ability to *maintain* anonymity threaten to chill activity that falls within the core protections of the First Amendment.[93] As one Texas Court of Appeals opined, while it is well settled that speakers have free-speech rights to engage in anonymous speech, such a right would be "of little practical value if there was no concomitant right to *remain*

88. *Id.* at 578.

89. *Id.* at 575, 580–81.

90. *Id.* at 578–80.

91. *Id.* at 578–81.

92. *See supra* Sections II.B–C.

93. *See, e.g.*, NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 462–63 (1958) (finding that compulsory disclosure of the names of individuals engaging in activity protected under the First Amendment impermissibly created a "likelihood of a substantial restraint" upon the exercise of protected activity that could result in a "repressive effect").

anonymous after the speech is concluded."[94] In this context, "[T]he chilling effect on the First Amendment right of free speech that results from making such 'confidential' information [e.g., an anonymous speaker's identity] too easily accessible is apparent."[95]

Courts are still obligated to balance the rights of injured plaintiffs seeking to uncover anonymous wrongdoers with those of defendants exercising their right to anonymous speech on the internet.[96] As such, many courts require plaintiffs to make a threshold showing before permitting discovery into an anonymous internet speaker's identity.[97] Lacking US Supreme Court guidance on the issue, jurisdictions typically adopt one of two approaches: either the *Dendrite* or *Cahill* test.[98]

A. The Dendrite *Approach: An Overlarge Aegis*

Though *Seescandy.com* came earlier, the New Jersey Superior Court created the first test that maintained national traction in *Dendrite International, Inc. v. Doe No. 3*.[99] In *Dendrite*, Dendrite International brought a defamation claim against anonymous internet speakers for messages posted on a forum.[100] The messages alleged that Dendrite's president secretly, but unsuccessfully, attempted to sell the company.[101] Dendrite sought discovery compelling the forum's ISP to disclose the defendants' identities, but the court denied the company's subpoena to disclose the identity of the anonymous speakers after crafting a new test based on *Seescandy.com*.[102]

The court relied on *Talley* and *McIntyre* to support a speaker's right to anonymity and *Reno* to extend this right to internet speech.[103] In an attempt to balance Dendrite's right to recover for its alleged injury with the defendants' rights to anonymous internet speech, the court

---

94. *In re* Does 1–10, 242 S.W.3d 805, 820 (Tex. App. 2007) (emphasis added) (citing Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001)).

95. *Id.* at 821.

96. *Id.* at 820 ("The courts must balance the right to communicate anonymously with the right to hold accountable those who engage in communications that are not protected by the First Amendment.").

97. *See, e.g.*, Best W. Int'l, Inc. v. Doe, No. CV–06–1537–PHX–DGC, 2006 WL 2091695, at *4 (D. Ariz. July 25, 2006); Doe v. Cahill, 884 A.2d 451, 463 (Del. 2005); Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756, 760–61 (N.J. Super. Ct. App. Div. 2001).

98. *See infra* Sections II.A–B.

99. *Dendrite Int'l, Inc.*, 775 A.2d 756.

100. *Id.* at 760.

101. *Id.* at 763.

102. *Id.* at 763–64, 766–68, 772; *see also supra* Section I.F.

103. *Dendrite Int'l, Inc.*, 775 A.2d at 765.

applied the following balancing test: to uncover an anonymous internet speaker, plaintiffs must (1) undertake efforts to notify the anonymous posters that they were the subject of a subpoena or application for an order of disclosure and provide reasonable opportunity to oppose the application, (2) identify and "set forth the exact statements purportedly made by each anonymous poster that the plaintiff alleges constitutes actionable speech," and (3) set forth a prima facie case against the anonymous defendants by producing evidence for each element of the cause of action.[104] Finally, the court must balance each prospective defendant's First Amendment right of anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure of the defendant's identity.[105] The court ultimately affirmed the trial court's denial of Dendrite's discovery request because Dendrite failed to demonstrate that its injury was sufficiently connected to the defendants' action, thus failing the balancing test.[106]

Many courts follow the test put forth by *Dendrite* and relay their interpretations of what should be considered within each factor. For example, the Southern District of New York utilized the *Dendrite* test in *Sony Music Entertainment, Inc. v. Does 1–40*.[107] In *Sony*, Sony sued to discover the identity of forty individuals that it alleged downloaded, posted, and shared pirated music on the internet.[108] Citing the *Dendrite* test, the court divided out the test in a slightly different fashion, requiring that plaintiffs show: (1) a prima facie case of copyright infringement, (2) a sufficiently specific discovery request, (3) a demonstration of an absence of an alternative means to obtain the subpoenaed information, (4) a demonstration that the subpoenaed information is central to the plaintiffs' claim, and (5) that plaintiffs' alleged injuries outweigh the defendants' reasonable expectations of privacy under the First Amendment.[109] The court granted discovery because "defendants' First Amendment right to remain anonymous [gave] way to plaintiffs' right to use the judicial process to pursue what appear to be meritorious copyright infringement claims."[110] Ultimately,

---

104. *Id.* at 760.

105. *Id.* at 760–61.

106. *Id.* at 772.

107. Sony Music Entm't, Inc. v. Does 1–40, 326 F. Supp. 2d 556, 563–64 (S.D.N.Y. 2004).

108. *Id.* at 558.

109. *Id.* at 565–66.

110. *Id.* at 567. For other examples of courts that adopted and modified the *Dendrite* standard, see *In re* Ind. Newspapers Inc., 963 N.E.2d 534, 552 (Ind. Ct. App. 2012) (adopting a modified *Dendrite* standard); Indep. Newspapers, Inc. v. Brodie, 966 A.2d 432, 457 (Md. 2009) (adopting *Dendrite*); Mortg. Specialists, Inc. v. Implode-Explode Heavy Indus., Inc., 999 A.2d 184, 193 (N.H. 2010) (adopting *Dendrite*).

this test favors anonymous defendants because the higher burden placed on plaintiffs insulates trial court decisions from appellate review.[111]

B. The Cahill *Approach: A Plaintiff-Friendly Paper Tiger*

Not all courts choose to follow *Dendrite*. Nearly as popular is the *Cahill* approach, developed by the Delaware Supreme Court in *Doe v. Cahill*.[112] In *Cahill*, an elected official sued to unmask four anonymous defendants who posted comments concerning his "mental deterioration" and "paranoia."[113] While determining whether to grant Cahill's motion for discovery, the court devoted several pages of its opinion to analyzing the *Dendrite* test.[114]

In the end, the court found that only prongs one and three of the test merited adoption, requiring plaintiffs to go through reasonable efforts to notify potential defendants of suit and provide a prima facie case supporting the cause of action.[115] It explicitly rejected the second and fourth requirements as unhelpful, requiring plaintiffs to put forth the exact speech they found objectionable and using a final balancing test.[116] Specifically, it found that the second requirement "is subsumed" by the third because, to present a prima facie case, the plaintiff would "necessarily" need to quote the defendant's actionable language.[117] Moreover, it found the final balancing test "unnecessary" because the court believed that it "adds no protection above and beyond that of the [prima facie requirement] and needlessly complicates the analysis."[118] In analyzing the two remaining factors, the court implemented a summary judgment standard.[119] Ultimately, the court found Cahill's claim lacked merit and remanded the case with instructions to dismiss his claim.[120] This approach, designed to weed out only "silly or trivial claims," is plaintiff-friendly because it imposes a lesser burden than the

111. *See, e.g.*, Melvin v. Doe, 836 A.2d 42, 50 (Pa. 2003) (deferring to the trial court's discretion in denying discovery of the defendant's identity after adopting *Dendrite*). *But see* Doe I v. Individuals, 561 F. Supp. 2d 249, 254–57 (D. Conn. 2008) (employing *Dendrite* but ultimately granting discovery into the defendant's identity)

112. Doe v. Cahill, 884 A.2d 451 (Del. 2005).

113. *Id.* at 454.

114. *Id.* at 459–60.

115. *Id.* at 461.

116. *Id.*

117. *Id.*

118. *Id.*

119. *Id.* at 460.

120. *Id.* at 468.

Dendrite test by eliminating two of its four elements.[121] Thus, most cases that use this standard ultimately expose the defendant's identity.[122]

C. The Intellectual Property Exception: Sinking Masked Pirates in the IP High Seas

Though one test is more cumbersome than the other, both still burden plaintiffs that want to unmask anonymous internet speakers, but that pressure can be case specific. Many jurisdictions hold that US Supreme Court precedent and property rights concerns indicate that plaintiffs seeking action against anonymous IP infringers should benefit from a presumption in favor of unmasking the defendant in these cases.[123] This is because, according to the Southern District of New York, "the Supreme Court . . . has made it unmistakably clear that the First Amendment does not shield copyright infringement."[124] The Fifth Circuit agreed in *Dallas Cowboys Cheerleaders v. Scoreboard Posters*, cautioning infringers that "[t]he first amendment is not a license to trammel on legally recognized rights in intellectual property."[125]

Confronting defendants that published software on their website allowing users to decrypt and download major motion pictures, the court in *Universal City Studios, Inc. v. Reimerdes* saw the case as "another step in the evolution of the law of copyright occasioned by advances in technology."[126] Even in 2000, the court noted that Congress had repeatedly found that "[c]opyright and, more broadly, intellectual property piracy are endemic [on the internet]."[127] The court continued, explaining that "[t]o the extent there is any tension between free speech

---

121. *Id.* at 459.

122. *See, e.g.*, Getaway.com LLC v. Does, No. CV 15–531–SLR, 2015 WL 4596413, at 2–3 (D. Del. July 30, 2015) (adopting *Cahill*, finding that the plaintiffs satisfied their burden, and granting the plaintiffs discovery into the defendant's identity); Best W. Int'l, Inc. v. Doe, No. CV–06–1537–PHX–DGC, 2006 WL 2091695, at *4, 6 (D. Ariz. July 25, 2006) (adopting *Cahill* and granting discovery into the defendant's identity); *cf.* Salehoo Group, Ltd. v. ABC Co., 722 F. Supp. 2d 1210, 1216, 1218 (W.D. Wash. 2010) (rejecting the *Cahill* formulation and quashing the plaintiff's motion seeking to unmask the defendant).

123. *See* Cable/Home Commc'n Corp. v. Network Prods., Inc., 902 F.2d 829 (11th Cir. 1990); Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211 (S.D.N.Y. 2000).

124. *Universal City Studios, Inc.*, 82 F. Supp. 2d at 220 (citing Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 555–60 (1985)).

125. Dallas Cowboys Cheerleaders, Inc. v. Scoreboard Posters, Inc., 600 F.2d 1184, 1188 (5th Cir. 1979) (citing Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562, 577 n.13 (1977)).

126. *Universal City Studios, Inc.*, 82 F. Supp. 2d at 213.

127. *Id.* at 225 (footnote omitted).

and protection of copyright, the [Supreme] Court has found it to be accommodated fully by traditional fair use doctrine."[128]

Ten years earlier, the Eleventh Circuit confronted a nearly identical issue in *Cable/Home Communication Corp. Network Productions, Inc.*[129] In *Cable Communication*, the defendant created software that allowed users to pirate HBO programming by decrypting the satellite signal used to broadcast it.[130] Agreeing with the Fifth Circuit that "[t]he first amendment is not a license to trammel on legally recognized rights in intellectual property,"[131] the Eleventh Circuit found that the carrying out and facilitation of piracy was far outside the First Amendment's protections.[132]

The practical realities surrounding internet IP infringement make utilizing this exception crucial. As the World Intellectual Property Organization noted, "[T]he fastest growing area of counterfeit trade is online."[133] Over $133 billion alone was spent online on counterfeit products in 2009, a number that has grown over the past decade.[134] Arguably, the most valuable asset that a company has is its "brand," particularly in the contexts of launching initial public offerings and completing mergers and acquisitions.[135] Indeed, "[t]ime is of the essence as each minute that an infringing site operates exponentially increases the risks that the targeted brand will suffer irreversible damage."[136] Plaintiffs who cannot unmask infringing defendants in a timely manner may find it to be too little, too late for their bottom line when a court finally grants discovery into an infringer's identity. Courts can prevent such losses by adopting the IP exception into an unmasking framework.

The damage that anonymous internet infringement inflicts on the economy supports adopting the exception as well. The US Department of Commerce estimates that the domestic value of stolen intellectual property is between $200 billion and $250 billion

---

128. *Id.* at 220 (footnote omitted).

129. *Cable/Home Commc'n Corp.*, 902 F.2d 829 (11th Cir. 1990).

130. *Id.* at 834.

131. *Id.* at 849 (quoting Dallas Cowboys Cheerleaders, Inc. v. Scoreboard Posters, Inc., 600 F.2d 1184, 1188 (5th Cir. 1979)).

132. *Id.* at 850.

133. Jochen M. Schaefer, *IP Infringement Online: The Dark Side of Digital*, WIPO: MAG. (April 2011), https://www.wipo.int/wipo_magazine/en/2011/02/article_0007.html [https://perma.cc/979D-NXG5].

134. *Id.*

135. *Id.*

136. *Id.*

annually.[137] Some industries, such as entertainment and software, are hit hard by such theft.[138] The Department of Commerce found that these industries and others like them have suffered losses in excess of $58 billion annually due to online copyright piracy alone.[139] Indeed, the Department of Commerce found that 27.7 percent of Americans work in fields that rely intensely upon IP protection to remain profitable.[140] "Without IP rights protection, others can profit from the sunk costs of others, putting the innovator at a disadvantage" and subjecting both the innovator and the market to substantial economic loss.[141] The fact that many pirates know better than to fly their flag and employ technology that makes it very difficult to locate them in the real world only complicates the matter.[142]

Piracy in the high seas of the international market has similarly disturbing implications on national economic security.[143] The US International Trade Commission estimates that Chinese theft of US intellectual property alone amounts to a loss of nearly $48 billion, leading to a loss of almost one million US jobs.[144] Total job losses from IP theft range from 3.8 to 4.8 million jobs.[145] Implementing the presumption in favor of unmasking defendants when plaintiffs assert infringement claims is based in both strong legal precedent and a compelling need to protect and enrich the US economy.

The internet makes it incredibly easy for wily defendants to anonymously infringe on intellectual property, draining millions of jobs and billions of dollars from the economy.[146] As discussed in Section I.E, it is difficult for plaintiffs to attempt to locate anonymous internet infringers when courts grant discovery into their identity.[147] By implementing the IP exception in unmasking analyses, the legal system can help innovators protect their creations and keep US jobs and dollars in the hands of US citizens.

---

137. Reggie Ash, *Protecting Intellectual Property and the Nation's Economic Security*, LANDSLIDE, May–June 2014, at 20, 21.

138. *Id.* at 22.

139. *Id.*

140. *Id.* at 21.

141. *Id.* at 21–22.

142. See discussion of the practical difficulties surrounding unmasking anonymous users *supra* Section I.E.

143. Ash, *supra* note 137, at 22.

144. *Id.*

145. *Id.* at 23.

146. *See id* at 20–22.

147. *See supra* Section I.E.

D. High Noon: The Unmasking Showdown in Texas

The problems surrounding the use (and abuse) of discovery to unmask anonymous internet speakers came to a head in Texas because of an interaction between Texas's anti-SLAPP statute, the Texas Citizens Participation Act (TCPA),[148] and Texas Rule of Civil Procedure 202 ("Rule 202").[149] Plaintiffs appear to be using Rule 202 as a loophole to circumvent the TCPA and "SLAPP" anonymous internet speakers with meritless suits.[150] These cases illustrate the real-world effects that unmasking efforts can have on anonymous speakers—namely, forcing them to endure behavior that anti-SLAPP statutes were designed to curtail.[151]

The TCPA provides that "[i]f a legal action is based on, relates to, or is in response to a party's exercise of the right of free speech . . . that party may file a motion to dismiss the legal action."[152] The statute defines a legal action as "a lawsuit, cause of action, *petition*, complaint, cross-claim or counter-claim or any other judicial pleading or filing that requests legal or equitable relief."[153] When a party files a TCPA motion to dismiss, all discovery into the legal action must cease until the court rules on the motion to dismiss.[154] Rule 202 allows plaintiffs to file a "petition" in court for limited pre-suit discovery "to investigate a potential claim or suit."[155] Since serving an anonymous internet speaker directly is often impossible, many plaintiffs serve the petition on service providers and website owners in an attempt to reveal the speaker's identity without having to file an actual "suit" that triggers the TCPA.[156] As discussed below, while some Texas courts recognize that the TCPA clearly applies to Rule 202 vis-à-vis the statute's use of the word "petition," others unfortunately fail to see this clear textual application.

---

148. *See* TEX. CIV. PRAC. & REM. CODE ANN. §§ 27.001–.011 (West 2018).

149. TEX. R. CIV. P. 202.1.

150. *See, e.g.*, DeAngelis v. Protective Parents Coal., 556 S.W.3d 836 (Tex. App. 2018); Glassdoor, Inc. v. Andra Grp., LP, 560 S.W.3d 281 (Tex. App. 2017), *vacated*, 575 S.W.3d 523 (Tex. 2019); *In re* Elliott, 504 S.W.3d 455 (Tex. App. 2016).

151. *See* discussion *supra* Section I.D.

152. TEX. CIV. PRAC. & REM. § 27.003(a).

153. TEX. CIV. PRAC. & REM. § 27.001(6) (emphasis added).

154. TEX. CIV. PRAC. & REM. § 27.003(c).

155. TEX. R. CIV. P. 202.1 (emphasis added).

156. *See DeAngelis*, 556 S.W.3d 836; *Glassdoor, Inc.*, 560 S.W.3d 281; *In re Elliott*, 504 S.W.3d 455.

1. *In re Elliot*

In 2016, the Texas Third Court of Appeals in Austin examined the interaction between the TCPA and Rule 202 in *In re Elliot*.[157] In *In re Elliot*, a user writing under the pseudonym of "The Pump Stopper" published an article negatively reflecting on the financial prospects of MagneGas, a Delaware corporation headquartered in Florida.[158] MagneGas filed a Rule 202 petition in response, alleging that Elliot was affiliated with the article because he owned a website by the name of "PumpStopper" and believed he could help find the article's author.[159] Instead of scheduling a hearing to serve Elliot with the petition, MagneGas served Elliot with a subpoena for a deposition based solely on its Rule 202 petition without obtaining an order authorizing it to do so.[160] After refusing to attend this deposition through counsel, Elliot filed several motions aimed at curtailing MagneGas's efforts to compel his compliance in revealing the anonymous speaker's identity.[161] Soon after, the user appeared as a John Doe and filed a TCPA motion to dismiss MagneGas's Rule 202 petition, asserting that its petition sought to curtail Doe's freedom of speech.[162] The trial court ultimately granted MagneGas's petition and ordered discovery into material "relating to the . . . article by PumpStopper" without ruling on Doe's TCPA motion to dismiss.[163] Elliot responded by petitioning for mandamus relief to prevent pre-suit discovery, asking the court of appeals to compel the trial court to address Doe's TPCA motion.[164]

The court of appeals first noted that the issue was appropriate for mandamus consideration because Rule 202 petitions were ancillary to the possible subsequent suit and thus were neither final nor appealable.[165] In an attempt to stave off relief, MagneGas argued that the TCPA has no application to a Rule 202 proceeding.[166] Specifically, it argued that the TCPA's purpose is to "dispose of lawsuits," that a Rule 202 petition as a pre-suit discovery mechanism is not a lawsuit, and

157. *In re Elliot*, 504 S.W.3d 455.

158. *Id.* at 458.

159. *Id.*

160. *Id.*

161. *Id.*

162. *Id.* at 458–59.

163. *Id.*

164. *Id.*

165. *Id.* at 459. This issue is particularly concerning in the SLAPP context, as the harm from SLAPPs comes not from a possible settlement or judgment but from the fact that the plaintiff forced the defendant to hire counsel and go through the expensive litigation process to begin with. *See* discussion *supra* Section I.D.

166. *In re Elliot*, 504 S.W.3d. at 463.

that the word "petition" in the TCPA refers to a pleading that asserts a cause of action or a claim.[167]

The court noted that the entire purpose of the TCPA is "to encourage and safeguard the constitutional rights of persons to . . . speak freely . . . to the maximum extent permitted by law and, at the same time, protect the rights of a person to file meritorious lawsuits for demonstrable injury."[168] "The [TCPA] accomplishes its purpose by providing a mechanism for early dismissal of 'legal actions' that are based on a party's exercise of the right of free speech."[169] As a "filing that requests equitable relief" in the form of pre-suit discovery, the court found that Rule 202 petitions certainly fall within the ambit of legal actions that could potentially impact a person's freedom of speech.[170] Finding that the TCPA applied to Rule 202 petitions, the court ultimately held that the trial court abused its discretion by permitting prediscovery under Rule 202 without first ruling on Doe's TCPA motion to dismiss.[171]

2. *Glassdoor*

The Texas Fifth Circuit Court of Appeals in Dallas confronted the same legal question and similar facts in *Glassdoor Inc. v. Andra Group*.[172] In *Glassdoor*, ten anonymous users claiming to be current or former employees of Andra posted negative reviews on Glassdoor's website.[173] Unable to access these anonymous internet speakers directly, Andra filed a Rule 202 petition seeking to depose a Glassdoor representative in an attempt to unmask the users for suit.[174] Glassdoor and Does One and Two responded with TCPA motions to dismiss.[175] The trial judge, after reviewing affidavits and other evidence submitted by the parties, denied the TCPA motions to dismiss and partially granted the Rule 202 petition insofar as it related to two sets of reviews.[176] The reviews identified in the order were not those allegedly written by the Doe parties and, as such, Glassdoor and the Doe parties appealed.[177]

---

167. *Id.*

168. *In re Elliot*, 504 S.W.3d. at 460–61.

169. *Id.* at 463.

170. *Id.* at 464–65.

171. *Id.* at 465.

172. Glassdoor, Inc. v. Andra Grp., LP, 560 S.W.3d 281 (Tex. App. 2017), *vacated*, 575 S.W.3d 523 (Tex. 2019).

173. *Id.* at 285.

174. *Id.*

175. *Id.*

176. *Id.*

177. *Id.*

The court dismissed the Doe parties' claims as lacking in standing because the trial court did not permit discovery into their identities in particular.[178] The court addressed whether the trial court abused its discretion by granting Andra's Rule 202 petition and granting discovery despite the users' First Amendment right to speak anonymously.[179] Assuming without deciding that it would be appropriate to adopt the *Cahill* approach in unmasking cases,[180] the court found that there was sufficient evidentiary support to allow Andra discovery under Rule 202.[181] Notably, the court refused to determine whether the TCPA applies to Rule 202, despite Andra, like MagneGas above, arguing that it does not.[182]

By affirming the trial court, the appellate court allowed Andra significant discovery into the anonymous internet speakers connected with the two sets of reviews without filing a formal suit, because Rule 202 is a *pre-suit* mechanism.[183] By allowing Andra to utilize a Rule 202 petition in this way, the court effectively sanctioned the use of a Rule 202 petition as a back door to the TCPA.[184] Though the Supreme Court of Texas granted certiorari for this case, it entirely sidestepped the unmasking dilemma by vacating and dismissing the case on mootness grounds.[185]

3. *DeAngelis*

One year later, the Texas Second Court of Appeals in Fort Worth confronted similar issues in *DeAngelis v. Protective Parents Coalition*.[186] In *DeAngelis*, the Protective Parents Coalition (PPC) maintained a website and Facebook page where they posted what they purported to have observed in family court proceedings.[187] The PPC asserted "that in the process of litigating family law cases, judges, attorneys, and court staff abuse their power to the detriment of children" for their personal gain.[188] Many users posted vitriolic comments on both the PPC website

178. *Id.* at 285–86.

179. *Id.* at 292.

180. *Id.* (citing *In re* Does 1–10, 242 S.W.3d 805, 820 (Tex. App. 2007)) (analyzing and utilizing the *Cahill* unmasking approach).

181. *Id.* at 294.

182. *Id.*; *see also* Brief on the Merits of Respondent Andra Group, LP at 16, Glassdoor, Inc. v. Andra Grp., LP, 575 S.W.3d 523 (Tex. 2019) (No. 17–0463).

183. *Glassdoor, Inc.*, 560 S.W.3d at 294–95.

184. *See id.*

185. Glassdoor, Inc. v. Andra Grp., LP, 575 S.W.3d 523, 531 (Tex. 2019).

186. DeAngelis v. Protective Parents Coal., 556 S.W.3d 836, 842 (Tex. App. 2018).

187. *Id.* at 841.

188. *Id.*

and Facebook group.[189] A group of attorneys often mentioned on the website filed a Rule 202 petition seeking pre-suit discovery into the PPC, claiming a need to investigate a potential claim for defamation.[190] The PPC responded with a TCPA motion to dismiss, alleging that the attorneys were attempting to chill their exercise of freedom of speech by attempting to "discover" information already at their fingertips.[191] The trial court granted the PPC's motion to dismiss, which the attorneys promptly appealed.[192]

After holding that a plain textual reading of the TCPA and Rule 202 supports Rule 202 falling under the TCPA, the court analyzed whether the PPC's TCPA motion to dismiss was appropriate.[193] Since the PPC's website, Facebook page, and individual PPC members' social media accounts were general publications intended for general public consumption and the speech was of "significant public concern," the TCPA motion to dismiss was appropriate.[194] Thus, the court held that the PPC's TCPA motion to dismiss applied to the attorneys' Rule 202 petition.[195]

The court then examined whether the trial court correctly granted the TCPA motion to dismiss.[196] Specifically, it inquired whether the attorneys produced clear and sufficient evidence demonstrating that "the likely benefit of allowing the petitioner . . . to investigate a potential claim outweighs the burden or expense of the procedure" imposed on the respondent.[197] The court responded in the negative.[198] It first noted that Rule 202 relief was never intended for routine use and "may not be used to circumvent discovery limitations that would govern the anticipated suit."[199] Indeed, it found that "the document requests [contained within the petition] appear[ed] so draconian that they would not be allowed in an actual lawsuit."[200] It then found that the petition not only failed to explain why pre-suit discovery was necessary but the petition demonstrated that pre-suit discovery was "unnecessary because the Attorneys already [had] more than enough

189. *Id.* at 845–46.
190. *Id.* at 842.
191. *Id.* at 845.
192. *Id.* at 846–47.
193. *Id.* at 849.
194. *Id.* at 850–51.
195. *Id.* at 852.
196. *Id.* at 853.
197. *Id.* at 854.
198. *Id.*
199. *Id.* at 855 (citing *In re* Wolfe, 341 S.W.3d 932, 933 (Tex. 2011)).
200. *Id.* at 858.

information to file an action for defamation without resorting to Rule 202."[201]

The court also went through pains to address a topic not fully briefed by the parties: the petitioners' desire to use a Rule 202 petition to unmask anonymous speakers.[202] The court emphasized that the fact that the speakers *may* have been masked[203] was irrelevant to the fact that their speech merited First Amendment protection.[204] The court admonished potential Rule 202 petitioners that attempting to unmask anonymous internet speakers "through the mechanism of pre-suit discovery seems to tread on very dangerous ground, arguably circumventing the very purposes of anti-SLAPP legislation and long-established First Amendment protections."[205] "Just as Rule 202 cannot be used as a tool to circumvent the free speech protections of the TCPA," the court continued, "impermissible pre-suit document discovery should not be used as a tool to stifle or quash speech on matters of public concern, however much we disagree or dislike such speech, without the filing of a formal lawsuit."[206] Ultimately, the court affirmed the trial court's dismissal under the TCPA because the attorneys failed to demonstrate that their potential benefit outweighed the enormous costs pre-suit discovery would place on the PPC.[207]

4. Tying the Cases Together

In re Elliot, *Glassdoor*, and *DeAngelis* each demonstrated facets of the issues surrounding unmasking anonymous internet speakers. *In re Elliot* and *Glassdoor* squarely addressed the efforts that business plaintiffs go through to unmask anonymous defendants that allegedly defamed them.[208] These plaintiffs, like those in hypotheticals A and B, have an interest in unmasking the defendants whose statements may very well harm their bottom line and personal reputation. The defendants, like those in hypotheticals A and B, have an equal interest in maintaining their anonymity in asserting their First Amendment rights.

---

201. *Id.* at 857.

202. *Id.* at 857 n.10.

203. The court notes that, as to the speakers on the PPC's Facebook page, it was doubtful they were masked because "on Facebook one often associates their real name and a photograph of their face with their profile." *Id.*

204. *DeAngelis*, 556 S.W.3d at 857 n.10.

205. *Id.*

206. *Id.* at 858.

207. *Id.*

208. *See supra* Sections II.D.1–2.

DeAngelis addressed a different set of issues: the practical problems posed by a system that potentially allows plaintiffs easy access to an anonymous speaker's identity.[209] Inadequately protecting an anonymous internet speaker's identity, especially through pre-suit discovery mechanisms, subjects speakers to the very harm that anti-SLAPP statutes are supposed to prevent.[210] Moreover, it deprives them of the ability to make the kinds of important contributions to public fora that anonymous speech elicits.[211] The problem, of course, is in determining how to "balance the right to communicate anonymously" on the internet with "the right to hold accountable those who engage in communications that are not protected by the First Amendment."[212]

III. SOLUTION

Currently, many courts that have confronted plaintiffs seeking to unmask anonymous internet speakers have settled on either adopting or adapting one of two analyses: the *Dendrite* or *Cahill* approach.[213] Both of these approaches fail to appropriately balance the right to anonymous internet speech with the need to vindicate an injured plaintiff's rights by tilting the scale too far in one direction or the other.[214] Moreover, neither of these approaches consider the strong legal basis for and overwhelming practical importance of lowering the plaintiff's burden to unmask anonymous infringers. The test that best balances plaintiff and anonymous internet speaker interests is a *Dendrite* approach that implements a rebuttable presumption in favor of the plaintiff in IP infringement cases.

The current *Dendrite* test places a high burden on plaintiffs by imposing a three-part requirement that they (1) attempt to notify the anonymous speaker, (2) offer the exact statements that the anonymous speaker purportedly made that allegedly constitutes actionable speech, and (3) set forth a prima facie case against the anonymous defendants by producing evidence for each element of the cause of action.[215] This concludes with a balancing test whereby the court weighs the speaker's right of anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure of the speaker's

209. *See* discussion *supra* Section II.D.3.
210. *See* discussion *supra* Section II.D.3.
211. *See* discussion *supra* Section II.D.3; *see also supra* Section I.D.
212. *In re* Does 1–10, 242 S.W.3d 805, 820 (Tex. App. 2007).
213. *See supra* Sections II.A–B.
214. *See* discussion *supra* Sections II.A–B.
215. Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 2001).

identity.[216] Though the degree to which this test protects anonymous speakers is admirable, its current application is overbroad. Namely, it confers the same First Amendment protections to anonymous internet infringers as it does to anonymous internet speakers during its balancing analysis, a quality clearly at odds with Supreme Court precedent.[217]

Cahill, however, simultaneously over- and underprotects anonymous internet speakers. By eliminating the first and third portions of the *Dendrite* approach, *Cahill* was explicitly designed to weed out only "silly or trivial claims."[218] Instead, a "plaintiff must make reasonable efforts to notify the defendant and must satisfy the summary judgment standard."[219] At first, this appears to overprotect defendants because a summary judgment standard demands litigants present factual disputes sufficient to withstand dismissal.[220] Without so much as the defendant's identity, it seems difficult to imagine any plaintiff making a sufficient showing.[221] In reality, however, the *Cahill* approach is a paper tiger, a pared-down version of *Dendrite* that expressly eschews the necessity of weighing the plaintiff's interests in discovery with the speaker's right to anonymous internet speech.[222] As noted above, courts that utilize the *Cahill* approach are far more likely to grant discovery into the speaker's identity than those that implement *Dendrite*.[223]

Just because speech takes place on the internet does not deprive it of any of the protections that it would be afforded otherwise.[224] Indeed, the importance of protecting anonymous speech on the internet weighs in favor of adopting the *Dendrite* approach. Through pseudonyms or purely anonymous posts and messages, speakers can engage in incredibly valuable and meaningful forms of speech.[225] Speakers can openly participate in communities where they can seek support and give advice on sensitive social topics like divorce and

---

216. *Id.* at 760–61.

217. "[T]he Supreme Court . . . has made it unmistakably clear that the First Amendment does not shield copyright infringement." Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211, 220 (S.D.N.Y. 2000) (citing Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 555–60 (1985)); *see also supra* Section II.C.

218. Doe v. Cahill, 884 A.2d 451, 459 (Del. 2005).

219. *Id.* at 461.

220. *See* FED. R. CIV. P. 56.

221. Judge Tuaro observed as much while analyzing and ultimately rejecting the *Cahill* approach. *See* McMann v. Doe, 460 F. Supp. 2d 259, 267 (D. Mass. 2006).

222. *See id.* at 268.

223. *See* discussion *supra* Section II.B.

224. Reno v. ACLU, 521 U.S. 844, 870 (1997); *see also supra* Sections II.B–C.

225. *See* discussion *supra* Section I.D.

mental illness. They can be whistleblowers, exposing corporate and political wrongdoing. They can honestly review their experiences at stores and in businesses as both customers and employees.[226] Perhaps most importantly, they can give voice to political opinions that they would be afraid to put forth otherwise.[227]

The threats anonymous speakers face if unjustly unmasked are real. The most chilling example is doxing. Harrowing enough to merit being specifically addressed in a Department of Justice bulletin, victims of doxing are exposed to an "anonymous mob of countless harassers, calling their phones, sending them emails, and even appearing at the victim's home."[228] This threat has a particularly chilling effect on political speech, the most highly protected form of speech under the First Amendment,[229] because doxing efforts primarily target those expressing contrarian views.[230]

For example, members of the Young Conservatives of Texas at the University of Texas at Austin were doxed by an Antifa group simply for their membership status and "liking" of conservative pages on social media.[231] In response to the students' First Amendment exercise, the Antifa group posted the members' names, emails, photographs, and employer phone numbers online.[232] These posts vilified the students for their political beliefs and encouraged viewers to call the students' employers and attempt to get them fired.[233]

The Online Safety Modernization Act of 2017 (the "Act"), if it passes, will address doxing by criminalizing the knowing publication of a person's personally identifiable information with "the intent that the information will be used to threaten, intimidate, or harass any person, incite or facilitate the commission of a crime of violence against any person, or place any person in reasonable fear of death or serious bodily injury."[234] Indeed, Title III of the Act is called the "Interstate Doxxing Provision."[235] The fact that this bill exists suggests congressional

---

226. *See* discussion *supra* Section I.D.

227. *See* discussion *supra* Section I.D.

228. *See* Blanch & Hsu, *supra* note 73, at 5.

229. *See* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 339–40 (2010).

230. *See* Ellis, *supra* note 74.

231. Toni Airaksinen, *More Than 30 UT Students Doxxed for Crime of Being Conservative*, PJ MEDIA (Jan. 13, 2019), https://pjmedia.com/trending/more-than-30-ut-students-doxxed-for-crime-of-being-conservative/ [https://perma.cc/4GFL-2R8L].

232. *Id.*

233. *Id.*

234. Online Safety Modernization Act of 2017, H.R. 3067, 115th Cong. § 301 (2017).

235. *Id.*

acknowledgment that a doxing problem exists—one so severe as to merit criminal sanctions.[236]

Adopting the *Dendrite* approach better protects anonymous internet speakers from another threat: SLAPP suits.[237] Having too low of a burden in unmasking analyses allows plaintiffs to abuse a court's ability to grant discovery into an anonymous internet speaker's identity, allowing them to further draw out meritless litigation. Such a result sanctions a plaintiff's wrongful desire to chill protected speech.[238]

Moreover, such a result is directly contrary to the majority of states' judgment on the value of First Amendment protections. Many states have acknowledged just how valuable speech—anonymous and otherwise—is on the internet.[239] Currently, thirty-one states have anti-SLAPP statutes, and the common law in two others simulates these statutes.[240] These statutes, like the TCPA, typically allow defendants an expedited process through which they can petition the court to shut down suits that implicate their First Amendment rights.[241] Courts should adopt the *Dendrite* approach because it vindicates the majority position that SLAPP suits must be halted at the earliest stage possible by appropriately burdening SLAPP plaintiffs attempting to unmask anonymous internet speakers.

The *Dendrite* approach, though superior to the *Cahill* approach because it more appropriately protects an anonymous internet speaker's First Amendment rights, still falls short because it fails to acknowledge the difference between anonymous speech and anonymous IP infringement. Plaintiffs alleging the latter deserve a rebuttable presumption in their favor during the court's balancing analysis out of concern for property rights[242] and Supreme Court precedent that makes it "unmistakably clear" that the First Amendment "does not shield copyright infringement."[243]

Additionally, the practical considerations underlying anonymous IP infringement on the internet cannot be understated.

---

236. *See id.*

237. *See* discussion *supra* Section I.D.

238. *See* discussion *supra* Section I.D.

239. *See State Anti-SLAPP Laws*, PUB. PARTICIPATION PROJECT, https://anti-slapp.org/your-states-free-speech-protection/#reference-chart [https://perma.cc/2AK5-RVLR] (last visited Sept. 12, 2019).

240. *Id.*

241. *See, e.g.*, TEX. CIV. PRAC. & REM. CODE ANN. § 27.003(a) (West 2018) ("If a legal action is based on, relates to, or is in response to a party's exercise of the right of free speech . . . that party may file a motion to dismiss the legal action."); *see also supra* Section II.D.

242. Dallas Cowboys Cheerleaders, Inc. v. Scoreboard Posters, Inc., 600 F.2d 1184, 1188 (5th Cir. 1979).

243. Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211, 220 (S.D.N.Y. 2000).

First, "each minute that an infringing site operates [or that an infringing post remains accessible] exponentially increases the risks that the [plaintiff] will suffer irreversible damage."[244] Plaintiffs who cannot unmask infringing defendants in a timely manner may find it to be too little, too late when a court finally grants discovery into an infringer's identity. Implementing the IP exception's rebuttable presumption will speed the court's balancing analysis. This need for speed is doubly important considering how difficult it is for courts and counsel to uncover wily pirates hiding behind layers of encryption and misdirection.[245] As noted above, even unsophisticated infringers can make use of false emails, account names, and VPNs to hide their illicit activity in only a few minutes.[246] This change of pace may make all the difference for an injured plaintiff's need to staunch the flow of capital bleeding out because of a defendant's anonymous infringement.

Moreover, the costs associated with IP infringement are staggering—between $200 and $250 billion are lost each year to IP theft, a significant portion of which likely occurs anonymously on the internet.[247] Indeed, over a quarter of US citizens work in fields intensely dependent upon IP protection to remain profitable.[248] The threat posed by IP theft over the internet has international implications as well. Chinese theft of US intellectual property alone amounts to a loss of nearly $48 billion, leading to a loss of almost one million US jobs.[249] Ash estimates that the total losses from IP theft fall between 3.8 million and 4.8 million jobs.[250] By implementing the IP exception into the *Dendrite* analysis, courts can take a step toward helping innovators keep the profits of their hard work and rescuing the millions of jobs lost to IP infringement.

Thus, the altered *Dendrite* analysis proceeds as follows: to succeed in an unmasking claim, plaintiffs must (1) undergo reasonable efforts to notify the anonymous speaker of the impending unmasking attempt and possible suit, (2) offer the exact statements that the anonymous speaker purportedly made that allegedly constitute actionable speech, and (3) set forth a prima facie case against the anonymous speakers by producing evidence for each element of the cause of action.[251] The court will then weigh the speaker's right of

244. *See* Schaefer, *supra* note 133.
245. *See* discussion *supra* Section I.E.
246. *See* discussion *supra* Section I.E.
247. *See* Ash, *supra* note 137, at 21.
248. *See id.* at 22.
249. *Id.*
250. *Id.* at 23.
251. Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 2001).

anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure of the speaker's identity in pursuing the action.[252] If the plaintiff makes a prima facie case for IP infringement, the court should apply a strong rebuttable presumption in favor of unmasking the anonymous defendant when it conducts the balancing test.

IV. CONCLUSION

The problems posed by plaintiffs seeking to wrongfully unmask anonymous internet speakers are legion. These plaintiffs, like Andrew in hypothetical A, may want to use unmasking suits to "SLAPP" down meritorious criticism. Perhaps a plaintiff is offended by the anonymous speaker's political statements and wants to misappropriate the court's power to expose their identity in what may ultimately function as a form of legally sanctioned doxing.[253] At the same time, plaintiffs like Bryan in hypothetical B must be able to vindicate their interests when confronted with defamatory statements. The most popular approaches to unmasking, the *Dendrite* and *Cahill* analyses, fail to appropriately balance the right to anonymous internet speech with the need to vindicate an injured plaintiff's rights by simultaneously over- and underprotecting anonymous defendants. Moreover, neither of these approaches consider the strong legal basis for and overwhelming practical importance of lowering the plaintiff's burden to unmask anonymous infringers. This failure exposes plaintiffs like Chris in hypothetical C to a level of actual and potential economic injury that flies in the face of current case law and critical economic considerations.

Adopting a modified *Dendrite* analysis remedies these issues by providing a heavy rebuttable presumption in favor of unmasking anonymous IP infringers. This approach appropriately balances the strong First Amendment precedent that protects anonymous internet speech with the need to staunch the flow of capital bleeding from the US economy through IP theft. It also explicitly enforces the important legal distinction between anonymous internet speakers and anonymous internet infringers, which current analyses fail to do. In sum, courts should adopt the modified *Dendrite* analysis because it protects

252. *Id.* at 760–61.

253. See discussion of doxing *supra* Section I.E, Part III.

anonymous speakers while exposing wolves in free-speech clothing.

Nathaniel Plemons[*]

[*] JD Candidate, Vanderbilt University Law School, 2020; BA, Rhodes College, 2017. The Author would like to thank his family—Dr. Ralph, Zahira, and Joshua Plemons—for their unconditional love and support throughout his education and the writing of this Note. He is also grateful to Judge Mark T. Pittman, who served as not only a reader and advisor for this Note but as a mentor to the Author generally. Finally, many thanks to the board and staff of the *Vanderbilt Journal of Entertainment & Technology Law* for their insightful comments and refined editing assistance.