Fordham Urban Law Journal

Volume 44
Number 4 *Colloquium - Getting There From Here: An Exploration of Regionalism and Transportation in the United States*

Article 10

2017

Cybermobs, Civil Conspiracy, and Tort Liability

Winhkong Hua

CYBERMOBS, CIVIL CONSPIRACY, AND TORT LIABILITY

Winhkong Hua[*]

---

[*] Fordham University School of Law, J.D., 2017. I am grateful for all the help that Professor Aaron Saiger has provided me through this process. I thank my family and friends for putting up with me while I went through this writing process, and I thank the members of the *Fordham Urban Law Journal* for helping develop my ideas and fixing my citations.

INTRODUCTION

Cities are centers of culture, learning, and debate. These urban spaces provide a stage upon which discordant voices are brought together, where communities may form, and where ideas can clash.[1] The Internet is the new urban, where dissident voices can find refuge and where the world grows closer.[2] But even as the Internet draws people closer together and allows debate to flourish, the Internet creates new ways for people to harass and harm others.[3] So as exists in cities, structures must be created to safeguard individuals while maintaining the diversity and vibrancy that makes the space desirable.

The Internet allows individuals to be hurt in ways that simply did not previously exist. Several examples demonstrate the new types of harms that have become available when people use the Internet as a tool of harassment: from false accusations, gender discrimination, and inexplicable ire, to the scorning of people who tread past certain social norms. After the Boston Marathon Bombing, Sunil Tripathi was falsely accused on Reddit of being the Boston Bomber; his family received hundreds of threatening and anti-Islamic phone calls.[4] Reddit users from around the world trawled through news articles,

---

1. In the words of modern urban planning's mother, Jane Jacobs:

> [T]he differences that often go far deeper than differences in color—which are possible and normal in intensely urban life, but which are so foreign to suburbs and pseudo-suburbs, are possible and normal only when streets of great cities have built-in equipment allowing strangers to dwell in peace together on civilized but essentially dignified and reserved terms.

JANE JACOBS, THE DEATH AND LIFE OF GREAT AMERICAN CITIES 83 (1961).

2. *See, e.g.*, Weiyu Zhang, *Virtual Communities as Subaltern Public Spheres: A Theoretical Development and an Application to the Chinese Internet*, *in* CYBER BEHAVIOR: CONCEPTS, METHODOLOGIES, TOOLS, AND APPLICATIONS (Linda Johnston ed., 2014), ACADEMIA, https://www.academia.edu/2077992/Virtual_communities_as_subaltern_public_spheres_A_theoretical_development_and_an_application_to_the_Chinese_Internet [https://perma.cc/HU5W-JKKW]; Brenden Gallagher, *20 Internet Communities You Can't Unsee*, COMPLEX (July 17, 2013), http://www.complex.com/pop-culture/2013/07/20-internet-communities-you-cant-unsee/ [https://perma.cc/RD7Q-VF6J] .

3. *See, e.g.*, Amanda Hess, *For the Alt-Right, Message is in the Punctuation*, N.Y. TIMES (June 10, 2016), https://www.nytimes.com/2016/06/11/arts/for-the-alt-right-the-message-is-in-the-punctuation.html [https://perma.cc/SZ7D-T6KX] (discussing the growth of the alt-right and what they borrow from 4chan communities); Abby Ohleiser, *'We Actually Elected a Meme As President:' How 4chan Celebrated Trump's Victory*, CHI. TRIB. (Nov. 12, 2016, 8:00 AM), http://www.chicagotribune.com/bluesky/technology/ct-meme-president-4chan-trump-wp-bsi-20161112-story.html [https://perma.cc/B8XB-63YD].

4. Jay Caspian Kang, *Should Reddit Be Blamed for the Spreading of a Smear?*, N.Y. TIMES MAG. (July 25, 2013), http://www.nytimes.com/2013/07/28/magazine/should-reddit-be-blamed-for-the-spreading-of-a-smear.html [https://perma.cc/PJ5S-T9SK].

images, and social media only to misidentify Mr. Tripathi, who had committed suicide days before the Bombing.[5] Steven Rudderham received death threats and hateful comments after accusations that he was a pedophile spread through Facebook; he committed suicide soon after.[6] After posting feminist critiques of video games, Anita Sarkeesian cancelled speaking engagements because of bomb threats, had her website shut down by hackers numerous times, was accused of being a fraud and a liar, and received death and rape threats which included her address and the names of her family members.[7] Jessica Leonhardt was eleven when she faced the ire of a cybermob; in just a few hours after someone posted one of her videos on 4chan,[8] her real name, phone number, real address, and social networking accounts circulated the Internet; harassers spammed her networking accounts, prank-called her home, and threatened her life.[9] As Leonhardt's mother said, "We've had many, many death threats. We're afraid to leave the house. We're afraid to go to bed. We're sleeping in shifts, my husband and I am."[10] Walter Palmer, the dentist who killed Cecil the Lion, received a staggeringly large amount of online abuse that quickly turned into harassment as Internet users shared his address,

---

5. *Id.*; *see also* Traci G. Lee, *The Real Story of Sunil Tripathi, the Boston Bomber Who Wasn't*, NBC NEWS (June 22, 2015, 9:05 AM), http://www.nbcnews.com/news/asian-america/wrongly-accused-boston-bombing-sunil-tripathys-story-now-being-told-n373141 [https://perma.cc/G2B4-Z6C2].

6. Sam Webb, *Father 'Driven to Suicide After He Was Wrongly Accused of Being a Paedophile on Facebook,'* DAILYMAIL (May 23, 2013, 4:02 PM), http://www.dailymail.co.uk/news/article-2329453/Father-driven-suicide-accused-paedophile-Facebook.html [https://perma.cc/6QXM-2NB8].

7. *See* Nick Wingfield, *Feminist Critics of Video Games Facing Threats in 'GamerGate' Campaign*, N.Y. TIMES (Oct. 15, 2014), http://www.nytimes.com/2014/10/16/technology/gamergate-women-video-game-threats-anita-sarkeesian.html [https://perma.cc/3RGV-JPQ2]; *see also* Luke Malone, *A Breakdown of Anita Sarkeesian's Weekly Rape and Death Threats*, VOCATIV (Jan. 28, 2015, 1:11 PM), http://www.vocativ.com/culture/society/anita-sarkeesian-threats/ [https://perma.cc/DW8K-4W37].

8. 4chan is a large online forum that emphasizes the anonymity of its users and actively does not archive. Users do not have to register in order to participate in threads, and do not even need to input a screenname when posting. 4chan usage is free. *See F.A.Q.*, 4CHAN, http://www.4chan.org/faq [https://perma.cc/WQK7-EAL3].

9. Adrian Chen, *How the Internet Beat Up an 11-Year-Old Girl*, GAWKER (July 16, 2010, 2:02 PM), http://gawker.com/5589103/how-the-internet-beat-up-an-11-year-old-girl [https://perma.cc/3ND8-XSSR].

10. Adrian Chen, *11-Year-Old Viral Video Star Placed Under Police Protection After Death Threats (Updated)*, GAWKER (July 18, 2010, 4:07 PM), http://gawker.com/5590166/11-year-old-viral-video-star-placed-under-police-protection-after-death-threats [https://perma.cc/VCG5-3HER].

his phone number, uncovered information about his employees and his patients, and even vandalized his home.[11]

These victims share a few similarities. Something brought them into prominence and made them targets of abuse for thousands of faceless cybermob participants. Each of the people mentioned became the victim of a mob: condemned in public, their names dragged through the mud, their lives and families threatened.[12] American society has protections against this type of behavior in the physical world where harassment is criminalized, and threatening or defamatory behavior can be redressed in the courts.[13] Extrajudicial mob punishment is prohibited in the United States.[14] But these protections are inadequate when applied to the Internet, and therefore cybermob activity thrives in the digital world.[15] This Note addresses this type of behavior on two levels: first, by proposing a way for victims to recover their damages through a novel civil conspiracy cause of action and, second, by arguing that this new cause of action can be used to discourage cybermob participation.

Part I discusses Internet harassment, exploring both why it is a problem and why the civil courts are unable to provide an adequate remedy to address the problem. Part I also discusses the tort of civil conspiracy, its elements, and features. As civil conspiracy is a common law tort, which is different from jurisdiction to jurisdiction, Part I also lays out the specific form of civil conspiracy that this Note proposes to use to address cybermob harassment. Part II discusses

---

11. *See* Max Fisher, *From Gamergate to Cecil the Lion: Internet Mob Justice Is Out of Control,* VOX (July 30, 2015, 2:30 PM), http://www.vox.com/2015/7/30/9074865/cecil-lion-palmer-mob-justice [https://perma.cc/9LRC-JKBC]; Meg Wagner & Corky Siemaszko, *Cecil the Lion's Killer Walter Palmer Ramps Up Security After Vandals Strike Florida Vacation Home, Leave Pigs' Feet*, N.Y. DAILY NEWS (Aug. 5, 2015, 7:13 PM), http://www.nydailynews.com/news/national/vandals-strike-fla-vacation-home-cecil-lion-killer-article-1.2315241 [https://perma.cc/5QNT-T83W].

12. *See supra* notes 4-11 and accompanying text.

13. *See, e.g.*, 42 U.S.C. § 1983 (2012) (creating a civil remedy for harassment based on deprivation of rights); 47 U.S.C. § 223 (2012) (criminalizing harassment that uses telecommunications as its medium); 18 U.S.C. § 2261A (2012) (criminalizing stalking).

14. *See generally* 71 A.L.R.2d 875 (1960) (discussing the development of the common law crime of unlawful assembly).

15. Fisher, *supra* note 11; Jon Ronson, *How One Stupid Tweet Blew Up Justine Sacco's Life*, N.Y. TIMES MAG. (Feb. 12, 2015), http://www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html [https://perma.cc/CD33-LXP4] (describing how a racist tweet became viral, causing Ms. Sacco to become the target of cybermob harassment, lose her job, and need to remove her social media presence).

the specific problem of cybermob harassment and why the proposed civil conspiracy cause of action could address the problem. Part III examines one case of cybermob harassment, analyzing how the facts of the case fit the elements of civil conspiracy and extrapolating how similar facts in other cybermob harassment campaigns could also fit civil conspiracy elements. Part III also explores how one court has addressed the problem examined in Part II. This Note explores the contours of and gaps in current law, to find a way for victims of cybermob harassment to recover and to discourage cybermob participation.

I. BACKGROUND OF INTERNET HARASSMENT AND CIVIL CONSPIRACY

Before discussing cybermob harassment in particular and how civil conspiracy can be used to address it, this Note discusses the background and legal landscape that frames these issues. The unique terrain of the Internet underlies the difficulty in addressing cybermobs and cybermob harassment. Section I.A discusses Internet harassment generally, and how features inherent to the Internet make harassment there a challenging problem to address. Section I.B discusses why civil litigation is currently an inadequate remedy for victims of Internet harassment. Section I.C addresses civil conspiracy, and what features of civil conspiracy may be useful for Internet harassment victims attempting to recover damages in court.

A. Internet Harassment

Cyber harassment and cyberstalking are contemporary problems that courts and legislatures have only recently begun addressing.[16] Cyber harassment and cyberstalking are defined in a variety of ways, by scholars, statutes, and common usage.[17] This Note uses Professor Danielle Citron's definitions of cyber harassment and cyberstalking.[18]

---

16. The first federal cyberstalking legislation was passed in 2000. Naomi Harlin Goodno, *Cyberstalking, A New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 MO. L. REV. 125, 151 (2007). The first cyberstalking prosecution took place in 1999. Greg Miller & Davan Maharaj, *N. Hollywood Man Charged in 1st Cyber-Stalking Case*, L.A. TIMES (Jan. 22, 1999), http://articles.latimes.com/1999/jan/22/news/mn-523 [https://perma.cc/FF5L-29PB].

17. *See, e.g.*, Goodno, *supra* note 16, at 126 ("[T]here is not a universally accepted definition, cyberstalking involves the use of the Internet, e-mail, or other means of electronic communication to stalk or harass another individual").

18. This Note uses Professor Citron's definition because it is broad enough to encompass many different cyber harassment tactics, while at the same time emphasizing that cyber harassment is part of a course of conduct, and not a series of isolated events.

Cyber harassment is "the intentional infliction of substantial emotional distress accomplished by online speech that is persistent enough to amount to a 'course of conduct' rather than an isolated incident."[19] Cyberstalking has a narrower meaning: "an online 'course of conduct' that either causes a person to fear for his or her safety or would cause a reasonable person to fear for his or her safety."[20] This Note addresses both cyber harassment and cyberstalking when using the term Internet harassment, as both problems are "accomplished by similar means and achieve similar ends," especially in the context of the cybermob harassment campaigns that this Note addresses.[21] Usage of Internet harassment as a term also encompasses harassment outside of cyberspace, insofar as acts of physical world harassment stem from an online course of conduct.[22] Internet harassment encompasses tactics that resonate across both spaces, including defamatory speech, impersonation,[23] threats, and doxxing.[24] This Note treats these tactics as part of the

---

19. DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 3 (2014); *see also* Wingfield, *supra* note 7; Chen, *supra*, note 10; Fisher, *supra* note 11.

20. CITRON, *supra* note 19, at 3.

21. *Id.*

22. For example, the GamerGate harassment campaigns mostly occurred on the Internet and arose from an Internet controversy, but members of GamerGate called in bomb threats to local police stations where GamerGate targets were scheduled to speak. Wingfield, *supra* note 7. Some victims have cyberstalkers show up in their physical lives. Others are SWATted, a process where a harasser makes a false police report so that a victim becomes a target of police response. *See* Nick Wingfield, *Online 'Swatting' Becomes a Hazard for Popular Video Gamers and Police Responders*, N.Y. TIMES (Mar. 20, 2014), http://www.nytimes.com/2015/03/21/technology/online-swatting-becomes-a-hazard-for-popular-video-gamers-and-police-responders.html [https://perma.cc/7HU6-5MZL].

23. In this context, the definition of the act includes both identity theft resulting in an economic result, as well as imitating someone to embarrass them without any financial gain. *See, e.g.*, Miller & Maharaj, *supra* note 16. Defendant allegedly impersonated the victim online in an attempt to have the victim raped. Draker v. Schreiber, 271 S.W.3d 318, 321 (Tex. App. 2008). Defendants created a MySpace.com profile using the identity of their vice-principle, which included "her name, photo, and place of employment, as well as explicit and graphic sexual references." Defendants impersonated their vice-principal for the purpose of retaliating against her because she had punished them. There was no economic motive. Appellant's Brief, at 2, Draker v. Schreiber, 271 S.W.3d 318 (Tex. App. 2008) (No. 4-07-00692-CV), 2008 WL 965855.

24. *See, e.g.*, CITRON, *supra* note 19, at 4. Doxxing is the public posting of personal information that a victim would like to keep secret. *See, e.g.*, Caitlin Dewey, *How Doxing Went from a Cheap Hacker Trick to a Presidential Campaign Tactic*, WASH. POST (Aug. 12, 2015), https://www.washingtonpost.com/news/the-intersect/wp/2015/08/12/how-doxing-went-from-a-cheap-hacker-trick-to-a-presidential-campaign-tactic/ [https://perma.cc/A7MF-BJ76]; *Docs*, ENCYCLOPEDIA DRAMATICA,

course of conduct encompassed under Internet harassment and identifies distinctions between those tactics as they arise.

The Internet is an increasingly ubiquitous part of contemporary life. People are continually connected to the Internet, via cellphones, computers, and even by gaming consoles.[25] As Internet usage grows, bad behavior that uses the Internet as a medium also grows.[26] Internet harassment inflicts emotional, reputational, and pecuniary harm on its victims.[27] These harms are not confined to cyberspace; they carry over into the physical world, affecting not only the victims' presence online, but also in their day-to-day lives in the physical world.[28] Internet harassment makes some victims fear for their lives and the lives of their families.[29] Employers and educational institutions use the Internet to research employees, so that defamatory postings on the Internet can affect a victim's ability to obtain work or education.[30] Harassment campaigns can lead to

---

https://encyclopediadramatica.se/Doxing [https://perma.cc/H9SK-C52E] (last modified Apr. 25, 2017, 1:29 PM).

25. *See, e.g.*, Anna Debenham, *Testing Websites in Game Console Browsers*, A LIST APART (Sept. 11, 2012), https://alistapart.com/article/testing-websites-in-game-console-browsers [https://perma.cc/8QRA-USMZ].

26. *See* CITRON, *supra* note 19, at 12.

27. *See generally* CITRON, *supra* note 19; Jacqueline D. Lipton, *Combating Cyber-Victimization*, 26 BERKELEY TECH. L.J. 1103, 1112 (2011); *see also* Steve Henn, *Fixing Your Online Reputation: There's an Industry For That*, NPR: NAT'L PUB. RADIO (May 29, 2013, 5:49 PM), http://www.npr.org/sections/alltechconsidered/2013/05/29/187080236/Online-Reputation [https://perma.cc/2FL4-22VN].

28. Some commentators contrast cyberspace with "real-space." CITRON, *supra* note 19, at 4; *see also* Mattathias Schwartz, *The Trolls Among Us*, N.Y. TIMES MAG. (Aug. 3, 2008), http://www.nytimes.com/2008/08/03/magazine/03trolls-t.html [https://perma.cc/Y8HA-JULM] (using the term real life in contrast to Internet activities). This Note uses the term physical space, because using the term real as the antonym of cyberspace implies that cyberspace does not actually exist, or that cyberspace is imaginary. This Note considers both spaces distinct and real; just because interaction with cyberspace is mediated by technology does not mean that emotions, consequences, and relationships stemming from that interaction are any less genuine than those in the physical world.

29. *See* CITRON, *supra* note 19, at 3-4 (quoting Holly Jacobs, Internet harassment victim: "The revenge porn victim felt terrorized. 'I just feel like I'm now a prime target for actual rape . . . I never walk alone at night, and I get chills when I catch someone staring at me.'"); Keith Stuart, *Brianna Wu and the Human Cost of Gamergate: 'Every Woman I Know in the Industry is Scared*," GUARDIAN (Oct. 17 2014, 2:02 PM), http://www.theguardian.com/technology/2014/oct/17/brianna-wu-gamergate-human-cost [https://perma.cc/9CA8-4L9K] (describing GamerGate target who fled her home due to the doxxing of her personal information and subsequent threats she received).

30. CITRON, *supra* note 19, at 8 ("According to a 2009 Microsoft study, nearly 80 percent of employers consult search engines to collect intelligence on job applicants, and about 70 percent of the time they reject applicants due to their findings.");

emotional and psychological upset, up to and including suicide.[31] Trying to fix a negative online reputation can be difficult and expensive.[32] The upset in the lives of those affected by cyber harassment can be continuous because reputational harm is preserved on the Internet.[33] Internet harassment profoundly affects the lives of victims, even though some "might argue that online abuses are actually less serious than their offline analogs because the victim has the option of simply turning off the computer and walking away. However, in today's interconnected world that is not a viable option."[34] In modern life, it is almost impossible to avoid the Internet.

A victim's presence on the Internet is not divorced from their life in the physical world. The interconnectedness between cyberspace and physical space means that Internet harassment is harmful even when harassers choose to limit their course of conduct solely to cyberspace.[35] Though Internet harassment is similar to and related to

---

Daniel J. Solove, *Speech Privacy and the Internet*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 19 (Saul Levmore & Martha C. Nussbaum eds., 2012); Danielle Keats Citron, *How Cyber Mobs and Trolls Have Ruined the Internet—and Destroyed Lives*, NEWSWEEK (Sept. 19, 2014, 12:56 PM), http://www.newsweek.com/internet-and-golden-age-bully-271800 [https://perma.cc/9YVY-KUA3] ("A bank fired a financial sales consultant after someone impersonated her on a prostitution site, falsely suggesting her interest in having sex for money.").

31. CITRON, *supra* note 19, at 10-11 ("Cyber harassment victims struggle especially with anxiety, and some suffer panic attacks [as a result of their harassment]."); *see, e.g.*, Webb, *supra* note 6 (describing suicide due to false accusations of pedophilia, doxxing, and threats arising from the false accusation).

32. *See* Ann Bartow, *Internet Defamation as Profit Center: The Monetization of Online Harassment*, 32 HARV. J. L. & GENDER 383, 423-28 (2009) (describing a variety reputation defense tactics and businesses); Steven Henn, *Fixing Your Online Reputation: There's an Industry For That*, NPR: ALL TECH CONSIDERED (May 29, 2013, 5:49 PM), http://www.npr.org/sections/alltechconsidered/2013/05/29/187080236/Online-Reputation [https://perma.cc/F4LP-664G] (describing the online reputation industry).

33. Lipton, *supra* note 27, at 1112; *see also* Henn, *supra* note 27.

34. Lipton, *supra* note 27, at 1113; *see also* Last Week Tonight With John Oliver, *Online Harassment*, YOUTUBE (June 21, 2015), https://www.youtube.com/watch?v=PuNIwYsz7PI [https://perma.cc/KD8F-7HZF] (presenting a short segment highlighting cyber harassment and its effects on its victims).

35. Though some Internet harassment campaigns only take place on the Internet, many campaigns cross over into the physical world. This can take the form of bomb threats, harassing phone calls, and other tactics that are not confined to the Internet. CITRON, *supra* note 19, at 5. For example, the GamerGate campaigns started online, but quickly crossed into the physical world, with harassing phone calls and fake pizza deliveries. Brianna Wu, *Gamergate Death Threat is a Slam Dunk for Prosecutors. Will They Act?*, MARY SUE BLOG (May 20, 2015, 11:32 AM), http://www.themarysue.com/will-prosecutors-act-on-gamergate-death-threat/ [https://perma.cc/NLB5-

solely offline harassment or stalking, "despite facial similarities between physical abuses and cyber-abuses, there are significant underlying differences."[36] These differences include ease of access, group networking, persistence, and anonymity.[37] These features underlie both the impact of Internet harassment, as well as highlight the difficulties in addressing it.

First, ease of access contributes to the growth of Internet harassment and the development of mass Internet harassment campaigns.[38] Internet connections are increasingly available, allowing more and more people access to all the benefits and information that the Internet can provide.[39] In this Note, ease of access refers to the low bar to entry to participation in Internet harassment, both as a participant and as an observer. All that is required to make a defamatory website is an Internet connection, a few dollars, and a basic understanding of website design.[40] It is even easier to participate on online bulletin boards and social networking sites like 4chan,[41] Reddit,[42] or Facebook,[43] where the only barrier to

---

RDVR] (quoting a death threat she received in a phone call, "'I'm coming to your fucking house right now. I will slit your throat you stupid little fucking whore. I'm coming, and you'd better be fucking ready for me."); Cassandra (@ChrisWarcraft), TWITTER (Jan. 1, 2015, 1:47 PM), https://twitter.com/chriswarcraft/status/550770232877268992 [https://perma.cc/5MWV-V2TE] ("So #Gamergate just stiffed a pizza guy out of $30 because I wasn't home when they delivered the pizza. Ethics in screwing over bystanders!").

36. Lipton, *supra* note 27, at 1112.

37. CITRON, *supra* note 19, at 5; *see also* Mary Anne Franks, *Unwilling Avatars: Idealism and Discrimination in Cyberspace*, 20 COLUM. J. GENDER & L. 224, 255-56 (2011). This Note separates these features into distinct categories to more easily discuss their effects, but acknowledges that each of these features is interwoven. Ease of access allows for easier group formation, as does anonymity. Ease of access allows for the numbers that make anonymity viable.

38. Lipton, *supra* note 27, at 1113 ("[O]nline abusers can initiate and pursue their wrongful act inexpensively and easily from anywhere in the world.").

39. *Internet Use Over Time*, PEW RES. CTR. (Jan. 12, 2017), http://www.pewinternet.org/data-trend/internet-use/internet-use-over-time/ [https://perma.cc/TMR4-247U] (noting that "[t]oday, roughly nine-in-ten American adults use the internet.").

40. On goddaddy.com, a popular Internet hosting company, it costs $2.99 for a domain name and $4.99 for hosting. GODADDY.COM, https://www.godaddy.com/ [https://perma.cc/PPS3-R37D]. As for web design, basic WordPress themes are free, and there are numerous tutorials on how to put up a website. *See*, *e.g.*, Marc O'Dwyer, *Basic WordPress Tutorial*, YOUTUBE (Jan. 29, 2014), https://www.youtube.com/watch?v=IyJ_LQoCFMQ [https://perma.cc/36H5-VY2C].

41. There is no sign up necessary. One merely needs to go to the page, go to one of the specialty boards, such as /b/, click on a thread and can post. No name is required.

42. Reddit is one of the largest Internet forums. Users must register in order to participate in conversations, but there is no charge to register, and no registration is

participation is an Internet connection.[44] "Unlike any other medium, the Internet permits anyone with ideas, information, or a message to reach vast numbers of people,"[45] without regard to geography or access to traditional forms of media. The Internet is global, with users from almost every country on Earth[46] able to simultaneously reach other users regardless of physical distance.

Ease of access allows more and more people to form like-minded communities on the Internet. Networking tools such as Facebook, Twitter,[47] and Internet Relay Chat ("IRC")[48] connect groups of people together, which can both provide users a sense of community and can be a powerful organizing tool for social change.[49] These tools also allow groups who want to "troll"—Internet slang for the act of "intentionally disrupt[ing] online communities"[50]—to organize and spread their message just as easily.[51] Some Internet users find like-minded groups that polarize the views of group members, which in

---

required for those who only want to read. *About*, REDDIT, http://www.about.reddit.com [https://perma.cc/H7HY-SU4F].

43. Facebook is a large social media platform with a feature called a newsfeed, where certain posts receive more views as they become more viral. *About*, FACEBOOK, https://www.facebook.com/facebook [https://perma.cc/95AC-BVM2].

44. None of the three sites require payment to participate or to register basic accounts. Though Facebook has privacy settings, thereby allowing users to only view material from within their network, these privacy settings are optional.

45. Catherine E. Smith, *Intentional Infliction of Emotional Distress: An Old Arrow Targets the New Head of the Hate Hydra*, 80 DENV. U. L. REV. 1, 21 (2002).

46. Rachel Nuwer, *The Last Places on Earth without Internet*, BBC (Feb. 14, 2014), http://www.bbc.com/future/story/20140214-the-last-places-without-internet [https://perma.cc/PTZ8-JW8R].

47. Twitter is a popular microblogging site, where users can follow one another, and repost entries they find worthwhile reposting. *See About*, TWITTER, https://about.twitter.com/ [https://perma.cc/ZLP7-UBY7].

48. IRC stands for Internet Relay Chat, which is a computer application that facilitates chat communication between users. *See generally IRC*, WIKIPEDIA, https://en.wikipedia.org/wiki/Internet_Relay_Chat#IETF_RFC_1459 [https://perma.cc/B9YB-6YU3].

49. *See* Rebecca J. Rosen, *So, Was Facebook Responsible for the Arab Spring After All?*, ATLANTIC (Sept. 3, 2011), http://www.theatlantic.com/technology/archive/2011/09/so-was-facebook-responsible-for-the-arab-spring-after-all/244314/ [https://perma.cc/F5UX-6WL7] ("Facebook and elsewhere online is where people saw and shared horrifying videos and photographs of state brutality that inspired them to rebel. Second, these sites are where people found out the basic logistics of the protests—where to go and when to show up.").

50. Schwartz, *supra* note 28 (defining the term in the context of the trolls that the journalist interviewed and followed).

51. *See* Fisher, *supra* note 11 ("[S]ocial media platforms that allowed outraged web users to spread the story also enabled them to do more than just fume. It gave them the power to act on their anger, to reach into Palmer's life and punish him for what he'd done[.]").

turn fuels the rise of Internet abuse.[52] Social networking sites also provide a ready-made audience for harassment campaigns.[53] The Internet in general and social networks in particular give cyber harassment campaigns the ability to go viral,[54] because they allow for "near instantaneous, widespread dissemination."[55]

The persistence of information on the Internet means that even when victims disconnect from the Internet, they are unable to escape the results of their harassment. Search engine indexing[56] associates victims' names with the malicious online materials that harassers post; search engines make these materials both easily available and virtually persistent.[57] Victims are often unable to do anything about these results because search engine indexing is the result of complex algorithms that focus on relevance and popularity, rather than veracity.[58] These websites can last indefinitely; some forums store and index posts from the day the forum went up, preserving harassing content, such as libelous postings or false accusations, as long as the forum lasts.[59] The actual fact that an individual is a target of Internet

---

52. CITRON, *supra* note 19, at 62-63.

53. *See* Karen M. Bradshaw & Souvik Saha, *Academic Administrators and the Challenge of Social Networking Sites*, *in* THE OFFENSIVE INTERNET 143 (Saul Levmore & Martha C. Nussbaum eds., 2012) ("The number of potential group members is far greater than in physical communities; on Facebook, elementary school friends and potential employers may have access to the same information would previously have been available only to students in the academic setting.").

54. Viral or going viral is the process by which some piece of media spreads across the Internet via reposting and sharing. The term connotes mass sharing in a relatively short period of time. *See Viral*, TECHTERMS, http://techterms.com/definition/viral [https://perma.cc/U52H-XYYP] (last updated Feb. 9, 2011).

55. Nancy S. Kim, *Web Site Proprietorship and Online Harassment*, 2009 UTAH L. REV. 993, 1010 (2009); *see also* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 17-49 (2007) (discussing how quickly information spreads on the Internet).

56. Search engine indexing is the process by which search engine algorithms associate search queries and results, using information such as word association and number of visitors. *See Crawling & Indexing*, GOOGLE, https://www.google.com/insidesearch/howsearchworks/crawling-indexing.html [https://perma.cc/F2U4-YXUK].

57. Franks, *supra* note 37, at 256 ("[C]yberspace harassment can manifest much more readily. Particularly if the online attack is indexable by a major search engine like Google, it is accessible to almost anyone (the target's co-workers, fellow students, clients, children) almost anywhere (at her place of work, her school, her home, her doctor's office).").

58. Google-bombing is a technique that raises search prominence, which then associates a search term, such as a victim's name, with specific results. CITRON, *supra* note 19, at 69-70.

59. Paul J. Larkin, Jr., *Revenge Porn, State Law, and Free Speech*, 48 LOY. L.A. L. REV. 57, 62 (2014) ("The permanence of information on the Internet carries a past insult or injury forward, potentially forever, making an original sin into an eternal

harassment is itself catalogued and recorded, which in turn can act as another source of harassment.[60] Because of the global nature of the Internet, the bounds of geography are not nearly as relevant as they are in the physical world; victims' pasts follow them, even as they move physically.[61]

Lastly, even as the Internet brings victims into prominence, the Internet also allows harassers to hide behind a screen of anonymity. The Internet enables anonymous speech and expression. Even though anonymity on the Internet is usually not truly anonymous,[62] "[c]omputer-mediated interaction, however, occurs in a state of *perceived* anonymity," which in turn affects how users act online.[63] This promotes freedom of speech, removing barriers to speech by protecting authors from retaliation or social ostracism.[64] Speech often becomes more uninhibited, as it becomes divorced from the possibility of punishment.[65] However, this weakening of inhibitions can make users more likely to act in destructive ways and without the consideration of negative consequences on either themselves or others.[66] Individuals say things they would not say in their physical

---

one."). Reddit, for example, stores all of its non-moderator-deleted posts from 2005. These posts are searchable, both within Reddit itself, and as the result of a regular Google search. This Note's author searched himself in Google and found material from 2006, material that is not in any way within his control.

60. Take the example of Jessi Slaughter, one of the earliest well-documented examples of cybermob abuse. A Google search reveals a variety of information about her and the abuse she suffered in a variety of tones. *See, e.g.,* KnowYourMeme.com, *Jessi Slaughter*, KNOW YOUR MEME, http://knowyourmeme.com/memes/events/jessi-slaughter [https://perma.cc/2QLS-5LR7] (last updated July 16, 2014, 2:27 PM) (presenting coverage of that period in her life in neutral, academic terms); Chen, *supra* note 4 (presenting coverage in blog format from journalistic bloggers observing it as it happened); *Jessi Slaughter*, ENCYCLOPEDIA DRAMATICA, https://encyclopediadramatica.se/Jessi_Slaughter [https://perma.cc/9R9F-WRSP] (last updated June 3, 2017, 11:52 AM) (presenting coverage in mocking, trolling terms on a wiki, user-generated encyclopedia, that celebrates trolling).

61. Larkin, *supra* note 59, at 61.

62. For a fuller discussion of the types of anonymity available online, see Margot Kaminski, *Real Masks and Real Name Policies: Applying Anti-Mask Case Law to Anonymous Online Speech*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 815, 821-23 (2013).

63. CITRON, *supra* note 19, at 59.

64. Kaminski, *supra* note 62, at 821-22.

65. *Id.* at 828.

66. CITRON, *supra* note 19, at 57-59.

lives.[67] Others believe allegations at face value, spreading misinformation even though they mean well.[68]

The Internet and its unique features create a fertile ground for Internet harassment to flourish. However, because the problem of Internet harassment is relatively new, the law is not yet able to adequately address the needs of victims. Traditional methods of civil redress are currently insufficient as remedies, necessitating either change in the law or novel approaches to the problem.[69]

B. Civil Litigation and its Internet Inadequacies

It is difficult for unsophisticated, private victims of Internet harassment to use tort law and civil litigation as a remedy to Internet harassment.[70] Litigation is a time-consuming and resource-intensive endeavor.[71] Many people do not have the knowledge or resources to start the litigation process.[72] Internet-specific issues—including the (1) lack of defendants, (2) need to unmask possible defendants, and (3) jurisdictional issues—further exacerbate the expense and difficulty of litigation. This Section examines each issue in turn.

---

67. Daniel Zharkovsky, Note, *"If Man Will Strike, Strike Through the Mask": Striking Through Section 230 Defenses Using the Tort of Intentional Infliction of Emotional Distress*, 44 COLUM. J.L. & SOC. PROBS. 193, 214 (2010)

68. *See, e.g.,* Sarah Michael & Emily Crane, *One Thousand Times Over I Wish I Could Just Take It Back': Mum Who Shamed A Man As A 'Creep' On Facebook When He Was Taking A Darth Vader Selfie For His Kids Offers A Grovelling Apology*, DAILY MAIL (May 11, 2015, 12:11 AM), http://www.dailymail.co.uk/news/article-3076246/Mum-shamed-man-Facebook-taking-photos-kids-just-taking-Star-Wars-selfie-offers-grovelling-apology.html [https://perma.cc/Q56T-H52N].

69. *See* discussion *infra* Section I.B; *see also* CITRON *supra* note 19, at 120-41.

70. *See*, *e.g.,* CITRON, *supra* note 19, at 122-23; Lipton, *supra* note 27, at 1129.

71. *See* Paula Hannaford-Agor & Nicole L. Waters*, Estimating the Cost of Civil Litigation*, NAT'L CTR. FOR ST. CTS., 20 CT. STAT. PROJECT 1, 1 (2013), http://www.courtstatistics.org/~/media/microsites/files/csp/data%20pdf/csph_online2.ashx [https://perma.cc/R4S5-ECND] (examining median cost of different types of litigation).

72. *See* Marlisse Silver Sweney, *What the Law Can (and Can't) Do About Online Harassment,* ATLANTIC (Nov. 12, 2014), http://www.theatlantic.com/technology/archive/2014/11/what-the-law-can-and-cant-do-about-online-harassment/382638/ [https://perma.cc/5WZM-HED6]. The article notes that even though victims have the facts to support a variety of civil claims, victims often do not file suit: "unless you have Jennifer Lawrence's resources this isn't exactly realistic: Filing a case like this is a very expensive and time-consuming process, not to mention emotionally draining."). The most prominent case dealing with Internet harassment was handled *pro bono*. *See* Doe I v. Individuals (AutoAdmit), 561 F. Supp. 2d 249 (D. Conn. 2008).

1. Lack of Defendants

Plaintiffs in Internet harassment cases bring actions either to enjoin alleged defendants to take down harmful materials or to recover damages, but plaintiffs may have difficulty filing against the proper defendant. An example of enjoining alleged defendants is asserting a copyright claim against a website hosting revenge porn to take down the video on display; an example of recovering damages is an action attempting to recover for the distress or reputational harm suffered as a result of the harassment.[73] However, Internet harassment plaintiffs often cannot find a viable defendant against which to press a claim.[74] Two main factors explain why plaintiffs are often unable to find viable defendants: a) because interactive computer services ("ICSs") are generally unavailable as defendants, and b) because the Internet's ease of access and anonymity masks defendants' identities. This Note focuses on the recovery of damages rather than injunctive relief because the immunity of ICSs and the inability to pin down specific defendants from which tortious material originates renders injunctive relief difficult to receive.[75]

The ICS category includes website hosts, website proprietors, and Internet service providers ("ISPs").[76] ICSs are the most obvious litigation target for plaintiffs.[77] They are in the best position to remove defamatory or tortious material,[78] to limit the ability of harassers to access victims and audiences, and are the most easily identifiable potential defendants.[79]

Online content must pass through a number of ICSs before reaching a typical user.[80] As such, ICSs are intermediaries with a

---

73. CITRON, *supra* note 19, at 59.

74. Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 117 (2009).

75. *See* discussion *infra* Section I.B.1.

76. Michael D. Scott, *Would A "Right of Reply" Fix Section 230 of the Communications Decency Act?*, 4 J. INT'L MEDIA & ENT. L. 57, 57-58 (2012); 47 U.S.C. § 230(e)(2) ("'[I]nteractive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.").

77. Lipton, *supra* note 27, at 1132.

78. In this Note, the phrase "defamatory or tortious material" includes all actionable speech, including malicious falsehoods, threats, and personal information made public.

79. CITRON, *supra* note 19, at 168 (noting that ICSs control what content appears on their sites).

80. Because website hosts, proprietors, and Internet service providers are the intermediaries between content and its viewer, by very definition information must

degree of control over the material that passes through their hands.[81] ICSs control whether to host problematic material and can restrict harassers' access to platforms within the ICS's control.[82] Furthermore, ICSs are often the best tactical choice for lawsuits, as they are more likely than a random Internet user to have the money to pay for tort damages.[83] However, the Communications Decency Act of 1996 ("CDA"), particularly section 230(c), usually makes ICSs unavailable as defendants in civil suits.[84] Section 230(c) effectively immunizes ICSs from almost all civil liability arising from content originating with third parties.[85] As such, plaintiffs must look elsewhere for defendants, even when the ICS is a purveyor of the tortious material.[86] This is a sharp deviation from similar mediums in the physical world, where publishers "bear[] the same liability for the statement as if he or she had initially created it."[87] Where an offline publisher would be held liable for publishing a tortious editorial written by a third party, an ICS would not be similarly liable—even for hosting identical material.

CDA section 230(c) was a legislative response to *Stratton Oakmont, Inc. v. Prodigy Services, Co.*[88] Prodigy Services, the defendant, was an ICS that included a forum where users could post in discussion threads.[89] The plaintiff, an investment company that

---

pass through an ICS to reach the user. As a very simplified example, the process of viewing a picture means that the image's host server, which is an ICS, sends information through its ISP, which is another ICS, to the website where it is being viewed, which is an ICS, which is located on another host server, which can belong to yet another ICS.

81. David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 389-91 (2010) (discussing ICSs as intermediaries and conduits between content creators and audiences).

82. *See id.*, at 386.

83. ICSs like Facebook, Twitter, Reddit, and GoDaddy are all large corporate organizations more likely to have deep pockets compared to the low bar to entry for participation in Internet harassment. Bandwidth costs money; websites that contain more information or see more visitors are therefore more expensive to maintain. *See* Lipton, *supra* note 27, at 1131.

84. Lipton, *supra* note 27, at 1131-32.

85. 47 U.S.C. § 230(c)(1) (2000) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

86. Citron, *supra* note 74, at 116. For example, revenge porn sites are usually not liable for the material they post because the material originates from users of the site. CITRON, *supra* note 19, at 173-74.

87. Ardia, *supra* note 81, at 397.

88. No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

89. *Id.* at *1.

was discussed in one of the threads, sued Prodigy over allegedly defamatory postings made by the forum's users.[90] The court held that Prodigy was liable for publisher liability because Prodigy moderated content posted by its users, thereby exercising editorial control.[91] Congress responded with section 230(c).[92] The CDA and section 230(c) were both part of a Congressional effort to prohibit indecency on the Internet. Though the United States Supreme Court ruled most of the CDA's indecency provisions unconstitutional because the CDA's indecency provisions violated the First Amendment, section 230(c) remains good law.[93] Ironically, Prodigy was sued for trying to moderate and control the content posted by their users in order to create a family friendly environment; section 230(c) now allows ICSs to forgo control or moderation of user-generated content, which can lead to very family un-friendly content.[94]

Zeran v. America Online, Inc.[95] extended the reach of section 230(c) immunity to distributor liability,[96] effectively resulting in a virtually absolute immunization of ICSs from liability for user-generated content.[97] In *Zeran*, the plaintiff brought a negligence action against America Online ("AOL"),[98] alleging that AOL was negligent by unreasonably delaying the removal of a third party's defamatory posts.[99] Anonymous posters in an AOL-hosted forum linked the plaintiff's phone number and personal information with slogans in support of Timothy McVeigh and the Oklahoma City Bombing, thereby implying that the plaintiff was involved with

---

90. *Id.* The postings included allegations that the organization was a "cult of brokers who either lie for a living or get fired," and that some of the organization's securities offerings were "major criminal fraud" and "100% criminal fraud."

91. *Id.* at *2.

92. Ardia, *supra* note 81, at 409.

93. *See*, *e.g.*, CITRON, *supra* note 19, at 171.

94. Citron, *supra* note 74, at 115-16.

95. Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997), *cert. denied*, 524 U.S. 937 (1998).

96. Publisher liability references the common law concept that one who republishes libel is subject to liability as if she had originally published it. Restatement (Second) of Torts § 578 (1977). Distributors, such as a bookstore, are only liable for defamatory statements if they knew or should have known about the defamatory material. *Id.*

97. Ardia, *supra* note 81, at 465. User-generated content is content—anything from images to text—created by a website's users rather than its proprietors.

98. America Online is an Internet Service Provider that also hosts forums as well as email and news services. *Aol.com*, AOL, http://www.aol.com [https://perma.cc/U4JJ-MR6C].

99. *Zeran*, 129 F.3d at 329.

Timothy McVeigh.[100] The plaintiff then became the victim of Internet harassment, receiving hateful messages online and threats via telephone. The United States Court of Appeals for the Fourth Circuit held that there was no difference between distributor or publisher liability under section 230; ICSs are immunized against both when tortious material originates from third party content creators.[101] The plaintiff was therefore unable to recover from AOL, as the Fourth Circuit affirmed the district court's ruling that Mr. Zeran's claims were barred by section 230(c).[102] Other courts followed the *Zeran* reasoning, and were "consistent in holding that an intermediary's refusal to remove content after notification is protected by section 230, and even if the intermediary has actual knowledge of falsity, it will not be liable for the speech of third parties."[103] After *Zeran*, ICSs became virtually immune to liability for content created by their users.

There have been some recent developments that indicate a possible change in the scope of section 230(c) immunity. In *Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, the United States Court of Appeals for the Seventh Circuit suggested disagreement with *Zeran's* blanket immunity.[104] The plaintiffs brought a Fair Housing Act ("FHA") suit against Craigslist, alleging that Craigslist was responsible for user postings that violated the FHA.[105] In denying the claim, the Seventh Circuit's reading of section 230(c) relied on the absence of the word "immunity" in the

---

100. *Id.*

101. *Id.* at 331-32 ("[Distributor] liability is merely a subset, or a species, of publisher liability, and is therefore also foreclosed by § 230.").

102. *Id.* at 328.

103. Ardia, *supra* note 81, at 465.

104. 519 F.3d 666, 670-71 (7th Cir. 2008), *as amended* (May 2, 2008) ("Why not read § 230(c)(1) as a definitional clause rather than as an immunity from liability, and thus harmonize the text with the caption? See Carlisle v. United States, 517 U.S. 416, 421 (1996). On this reading, an entity would remain a 'provider or user'—and thus be eligible for the immunity under § 230(c)(2)—as long as the information came from someone else; but it would become a 'publisher or speaker' and lose the benefit of § 230(c)(2) if it created the objectionable information. The difference between this reading and the district court's is that § 230(c)(2) never requires ISPs to filter offensive content, and thus § 230(e)(3) would not preempt state laws or common-law doctrines that induce or require ISPs to protect the interests of third parties, . . . for such laws would not be 'inconsistent with' this understanding of § 230(c)(1). There is yet another possibility: perhaps § 230(c)(1) forecloses any liability that depends on deeming the ISP a 'publisher'—defamation law would be a good example of such liability—while permitting the states to regulate ISPs in their capacity as intermediaries.") (quoting Doe v. GTE Corp., 347 F.3d 655, 659-60 (7th Cir. 2003).

105. *Id.* at 668.

statute; the court further suggested that section 230(c) had a limited role, but did not say how limited that role was.[106] The court ruled against the plaintiff on the grounds that Craigslist was a messenger service, similar to FedEx or UPS, and could not be held liable for its users' violations, even if there was dicta suggesting what the limits of section 230(c) could be.[107]

In *Fair Housing Council of San Fernando Valley v. Roommates.com*, the United States Court of Appeals for the Ninth Circuit created an exception to section 230(c) immunity if the ISC "contributes materially to the alleged illegality of the conduct" that is the basis of the action.[108] Roommates.com was and is a roommate matching service; the plaintiff alleged that Roommates.com violated the FHA by posing questions during the user registration process that allowed its users to indicate an intent to discriminate.[109] The questions permitted users to exclude requests from other users based on race, gender, and marital status; users had to choose from a series of answers provided by Roommates.com.[110] The Ninth Circuit reasoned that Roommates.com became "much more than a passive transmitter of information provided by others; it [became] the developer, at least in part, of that information" by asking unlawful questions and providing unlawful, pre-populated answers.[111] The court further held that Roommates.com was liable as co-creator of the statements for its users' violations of the FHA.[112] Active authorship is distinct from passively providing a space in which users could express prohibited preferences without prompting from Roommates.com; the latter is still permissible.[113]

---

106. *Id.* at 669-70.

107. *Id.* at 668.

108. 521 F.3d 1157, 1168 (9th Cir. 2008).

109. *Id.* at 1164.

110. *Id.* at 1165-66 ("[T]he part of the profile that is alleged to offend the Fair Housing Act and state housing discrimination laws—the information about sex, family status and sexual orientation—is provided by subscribers in response to Roommate's questions, which they cannot refuse to answer if they want to use defendant's services.").

111. *Id.* at 1166.

112. *Id.*

113. *Id.* at 1165-66 (contrasting what is permissible—hosting information provided by users which may be in violation of the FHA—with what is not permissible—asking questions that violate the FHA to which users must provide answers or be unable to use the site).

The *Roommates.com* decision may have implications as to certain types of websites that foster harassing or discriminatory behavior.[114] These websites could include revenge porn sites, many of which are dedicated to disseminating private pornographic materials that their users submit.[115] A court could find that revenge porn sites materially contribute to their users' copyright infringement and other wrongful actions, and thereby should not be immune from liability.[116] Other ICSs that could be vulnerable to that exception could include 4chan[117] and Encyclopedia Dramatica. 4chan is a large online forum that emphasizes the anonymity of its users and actively does not archive; this has led to "/b/," a 4chan sub-forum, gaining a reputation as a hub for trolling and harassing behavior.[118] Encyclopedia Dramatica has entries on a number of cyber harassment campaigns; the tone of the entries is usually supportive of harassers and trolls, and entries on these campaigns include links to tortious material.[119] By posting links to or copies of tortious material, it raises the likelihood of tortious material appearing in search engine indexes.[120]

However, section 230(c) immunity and *Zeran* would still probably protect both sites from liability, even with the exception created in *Roommates.com*. The exception carved out by *Roommates.com* was very specific: by providing questions and answers that violated the

---

114. *See* Bradford J. Sayler, Note, *Amplifying Illegality: Using the Exception to CDA Immunity Carved Out by Fair Housing Council of San Fernando Valley v. Roommates.com to Combat Abusive Editing Tactics*, 16 GEO. MASON L. REV. 203 (2008).

115. CITRON, *supra* note 19, at 17; *see also* Jessica Roy, *Revenge-Porn King Hunter Moore, the 'Most Hated Man on the Internet,' Is Going to Jail*, NEW YORK (Feb. 19, 2015, 1:34 PM), http://nymag.com/daily/intelligencer/2015/02/revenge-porn-hunter-moore-jail.html [https://perma.cc/E2ST-YMCY] (describing the rise and fall of one of the most infamous revenge porn sites, "Is Anyone Up?").

116. CITRON, *supra* note 19, at 173-74.

117. *Id.* at 179.

118. *See* Adrien Chen, *The Art of Trolling: Inside a 4chan Smear Campaign*, GAWKER (July 17, 2010, 4:59 PM), http://gawker.com/5589721/the-art-of-trolling-inside-a-4chan-smear-campaign [https://perma.cc/T899-GPBF]; *see also* CITRON, *supra* note 19, at 179.

119. *See, e.g., Zoe Quinn*, ENCYCLOPEDIA DRAMATICA, https://encyclopedia dramatica.se/Zoe_Quinn [https://perma.cc/27L3-XCJB] (last updated Apr. 29, 2017, 9:09 PM).

120. *See* CITRON, *supra* note 19, at 69-70. More generally, popularity and number of visitors is used as part of search engine algorithms when associating queries and results. As such, a site that is visited more often when tied to a specific phrase will likely come up earlier in search results than a page tied to the specific phrase with less visits.

FHA, Roommates.com exposed itself to liability.[121] Though both "/b/" and Encyclopedia Dramatica celebrate Internet harassment and trolling culture, the websites are not set up to facilitate illicit behavior in the same way as Roommates.com.[122] Instead they provide open spaces where their users are able to post as they will; it is the users that make both sites what they are.[123] Though both sites do moderate to a certain extent, and that moderation could lead to a tone supportive of problematic behavior, such moderation merely regulates content created by third parties and is squarely within the ICS immunity granted by section 230(c).[124] Neither site actively provides the choice for users to participate in illicit behavior; their users post that type of material on their own, and the sites merely police that which is prohibited by law.[125]

There are various proposals to change the CDA to limit the protection that ICSs have under section 230(c). These are outside the purview of this Note, but include amending section 230(c) to: carve out specific types of bad behavior for liability;[126] create notice, take-down, and put-back procedures similar to the Digital Millennium Copyright Act;[127] and end immunity if the ICS receives actual "notice of objectionable content and fail[s] to take prompt remedial action to avoid further losses."[128]

2. Ease of Access and Anonymity

The easily accessible and anonymous nature of the Internet further exacerbates the dearth of possible defendants. As section 230(c)

---

121. Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1165-66 (9th Cir. 2008).

122. *See* CITRON, *supra* note 19, at 179 (discussing section 230(c)'s application to 4chan). Similarly, Encyclopedia Dramatica is a wiki—a user-generated encyclopedia—so it likely would not be considered facilitating illicit behavior because it is the users who generate the information on the site.

123. *See* Chi. Law. Comm. for Civ. Rts. Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 669-70 (7th Cir. 2008). Similar to Craigslist, these sites are messengers, and one cannot "sue the messenger just because the message reveals a third party's plan to engage in unlawful [behavior]." *Id.* at 672.

124. *See* CITRON, *supra* note 19, at 179;; *see also Roommates.com*, 521 F.3d at 1165-66.

125. *See FAQ*, 4CHAN, http://www.4chan.org/faq [https://perma.cc/6Q4Q-HADJ]; *see also About*, ENCYCLOPEDIA DRAMATICA, https://encyclopediadramatica.se/Encyclopedia_Dramatica:About [https://perma.cc/YD2T-MQA5] (last updated Mar. 23, 2017, 7:29 PM).

126. CITRON, *supra* note 19, at 177.

127. Scott, *supra* note 76, at 68 n.6.

128. David A. Myers, *Defamation and the Quiescent Anarchy of the Internet: A Case Study of Cyber Targeting*, 110 PA. ST. L. REV. 667, 686 n.33 (2006).

immunity removes ICSs from the possibility of suit, the nature of the Internet makes suing actual individual Internet users difficult. Participating in Internet harassment is inexpensive and mostly independent of geography.[129] There is no guarantee that there will be a defendant with enough money to compensate a plaintiff for the harm suffered.[130] Furthermore, ease of access creates jurisdictional issues, as a harasser can be "physically removed from the victim. He may be across the state, across the country, or even across the globe."[131] There might be no viable defendant for a plaintiff to file suit against, because all the potential defendants are either judgment-proof or inaccessible.[132]

In order to even attempt to recover damages, the plaintiff must be able to identify defendants. This is difficult to do considering the many layers of anonymity that may exist and that must be pierced before a defendant can be unmasked.[133] The most common way of identifying Internet users is via their internet-protocol ("IP") address, which ISPs issue to their users. Because ISPs are usually paid, the ISPs may have account information for the targeted user.[134] But to get the IP address, the plaintiff must subpoena the ISP for its IP address records.[135] The plaintiff must then match the records to the targeted IP and get the account information connected to that IP address from the ISP.[136] Some websites do not track or only

---

129. Posting on most forums is completely free. *See generally* Kim, *supra* note 55, at 1008.

130. *Id.*

131. Lipton, *supra* note 27, at 1113.

132. *See id.* Those who are judgment-proof are "unable to satisfy a judgment for money damages." *Judgment-Proof*, BLACK'S LAW DICTIONARY (10th ed. 2014).

133. *See* Kaminski, *supra* note 62, at 20-23.

134. However, there are also Internet users who splice into others' Internet access or use only publicly available access. The IP address would not matter then, because there would be no account information with which to identify the defendants. *See* Ben Rossi, *How A 7-Year-Old Girl Hacked A Public Wi-Fi Network In 10 Minutes*, INFO. AGE (Jan. 21, 2015), http://www.information-age.com/technology/security/123458891/how-7-year-old-girl-hacked-public-wi-fi-network-10-minutes#sthash.tv3YUxPU.dpuf [https://perma.cc/6N5Q-HJMB] (describing the ease with which a hacker can access other computers on a public Wi-Fi network and then use it for a man-in-the-middle attack). Man-in-the-middle attacks work by fooling the system into thinking that a given query comes from one computer with one IP address, rather than from another with a different IP address. *See Man-in-the-Middle Attack*, TECHOPEDIA, https://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm [https://perma.cc/A99N-4HSH].

135. *See infra* note 144.

136. Michael S. Vogel, *Unmasking "John Doe" Defendants: The Case Against Excessive Hand-Wringing over Legal Standards*, 83 OR. L. REV. 795, 853-54 (2004).

minimally track IP data to preserve user anonymity.[137] Even then, some potential defendants could be completely anonymous and untraceable via the use of a variety of tools, such as Tor, which "establishes anonymous Internet connections by funneling web traffic through encrypted virtual tunnels."[138] These tools make it almost impossible to track down a specific user without sophisticated software and high-powered computers.[139]

Assuming that the defendant is traceable, there are significant challenges for plaintiffs seeking to unmask defendants because of the First Amendment's protection of anonymous speech. In *McIntyre v. Ohio Elections Commission*, a case involving an Ohio statute that banned anonymous political solicitation, the United States Supreme Court held that the First Amendment protects anonymous speech.[140] The Court reasoned that anonymity was important to free speech, because it divorced messages from their speakers, encouraged a more active marketplace of ideas, and protected speakers from retaliation.[141] In *Reno v. ACLU*, the Court extended First Amendment protections to Internet speech.[142] Certain types of speech, such as true threats and defamatory speech, are not protected.[143]

In order to balance free speech concerns with plaintiffs' right to recover, courts use a variety of tests to determine whether it is appropriate for the court to issue a subpoena to unmask an anonymous defendant in a tort case.[144] The prima facie test comes

---

137. CITRON, *supra* note 19, at 165.

138. *Id.*

139. Though even Tor has its vulnerabilities, most people will not have access to the resources necessary to exploit those vulnerabilities. *See* Kevin Poulsen, *Visit the Wrong Website and FBI Could End Up in Your Computer*, WIRED (Aug. 5, 2014, 6:30 AM), http://www.wired.com/2014/08/operation_torpedo/ [https://perma.cc/G2ZN-VRDL] (detailing an FBI network investigative technique that can be used to track a Tor user).

140. 514 U.S. 334 (1995) (holding that an Ohio statute prohibiting anonymous political speech was unconstitutional.).

141. *Id.* at 341-42.

142. 521 U.S. 844, 870 (1997). The Court struck down parts of the Communications Decency Act meant to protect children from obscene or indecent material on the grounds that it was not narrowly tailored enough.

143. *See*, *e.g.*, Watts v. United States, 394 U.S. 705, 707 (1969) (distinguishing constitutionally protected speech from that which is not protected, such as a threat).

144. Robert G. Larson & Paul A. Godfread, *Bringing John Doe to Court: Procedural Issues in Unmasking Anonymous Internet Defendants*, 38 WM. MITCHELL L. REV. 328, 340-41 (2011). Cases that involve unmasking defendants who have violated intellectual property rights generally have a lower standard than those

from *Dendrite International, Inc. v. Doe No. 3,* in which a corporation tried to unmask a commentator who allegedly made defamatory postings regarding the plaintiff's financial health.[145] It requires plaintiffs make reasonable effort to notify anonymous users that they are being made a party to a civil action.[146] Plaintiffs must withhold action for a reasonable period so that the targeted user may file and serve opposition.[147] Most importantly, the prima facie standard requires that plaintiffs set forth the exact actionable speech and actions, as well as provide evidence of each element of their causes of action sufficient to establish a prima facie case.[148] Once the plaintiff presents a prima facie cause of action, the court balances the equities between the defendant's First Amendment rights, "the strength of the prima facie case presented and the necessity for the disclosure of the anonymous defendant's identity to allow the plaintiff to properly proceed."[149] Overall, the prima facie test creates an exacting standard that still allows the judge to exert a degree of discretion through the balancing test.

Doe v. Cahill, which involved allegedly defamatory statements made by anonymous defendants on a blog, set out the summary judgment standard.[150] This test is similar to the *Dendrite* test in that it requires reasonable efforts to notify the defendants that plaintiffs are seeking to join, and that plaintiffs withhold action until those efforts are made.[151] *Cahill* differs from *Dendrite* by requiring that plaintiff "support his defamation claim with facts sufficient to defeat a summary judgment motion."[152] The *Cahill* court found the balancing

---

for defamation. *See* Jeannie Roebuck, Note, *Bittorrent Sharing: The Case Against John Does*, 18 INTELL. PROP. L. BULL. 35, 42 (2013).

145. *See* Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756, 760 (N.J. Sup. Ct. App. Div. 2001); *see also* Ashley I. Kissinger & Katharine Larsen, *Untangling the Legal Labyrinth: Protections for Anonymous Online Speech*, 13 J. INTERNET L. 1, 18 (2010).

146. *Dendrite*, 775 A.2d at 760.

147. *Id.*

148. *Id.*

149. *Id.* at 760-61; *see also,* Greenbaum v. Google, Inc., 845 N.Y.S.2d 695 (Sup. Ct. 2007) (using the *Dendrite* test, and analyzing plaintiff's specified posts to determine if there was a valid cause of action); Doe I v. Individuals (AutoAdmit), 561 F. Supp. 2d 249, 254-55 (D. Conn. 2008) (applying *Dendrite*, and showing how each element is met by the facts of the case).

150. Doe v. Cahill, 884 A.2d 451, 460 (Del. 2005).

151. *Id.*

152. *Id. See also* Getaway.com LLC v. Does, No. CV 15-531-SLR, 2015 WL 4596413, at *2 (D. Del. July 30, 2015) (applying the *Cahill* test, noting that plaintiff provided a prima facie case sufficient to survive a summary judgment motion).

test unnecessary, as the weighing of the equities would already have occurred to survive the summary judgment test.[153]

Finally, the court in *Mobilisa, Inc. v. Doe,* where a plaintiff sought the identity of an anonymous email sender, kept the summary judgment *Cahill* standard, but also re-added the *Dendrite* balancing test. The court reasoned that the balancing test allowed judges to consider a wider array of factors and provided an additional safeguard by giving the court more discretion.[154]

Other tests exist, including the "good faith basis" standard, but the *Dendrite* prima facie, *Cahill* summary judgment, and *Mobilisa* hybrid tests are the most exacting and common of the tests used in unmasking.[155] In some states, such as California, plaintiffs must meet further requirements because of Strategic Lawsuits Against Public Participation ("SLAPP") statutes.[156] These statutes target frivolous lawsuits intended to chill anonymous speech on issues of public concern. These statutes create their own standards and challenges that plaintiffs must meet in addition to the previously discussed unmasking standards.[157]

3. Jurisdictional Issues

Jurisdiction is another hurdle for plaintiffs to face before they can have their day in court. The Internet is without borders; some defendants will be beyond the reach of United States courts. Some plaintiffs may be able to locate their defendants, but unable to establish personal jurisdiction.[158] To establish personal jurisdiction over an out of state defendant, the plaintiff must first ensure that the defendant and the cause of action fall within the forum state's long-arm statute, and then must satisfy the due process minimum contacts

---

153. *Cahill*, 884 A.2d, at 461 ("The fourth *Dendrite* requirement, that the trial court balance the defendant's First Amendment rights against the strength of the plaintiff's prima facie case is also unnecessary. The summary judgment test is itself the balance.").

154. Mobilisa, Inc. v. Doe, 170 P.3d 712, 720-21 (Ariz. Ct. App. 2007).

155. *See In re* Anonymous Online Speakers, 661 F.3d 1168, 1176 (9th Cir. 2011) ("The district court in this case applied the most exacting standard, established by the Delaware Supreme Court in *Doe v. Cahill*.").

156. Ardia, *supra* note 81, at 394.

157. *See, e.g.,* CAL. CIV. PROC. CODE § 425.16 (West 2015). Plaintiffs are "subject to a special motion to strike, unless the court determines that the plaintiff has established that there is a probability that the plaintiff will prevail on the claim."

158. *See* ALS Scan, Inc. v. Digital Serv. Consultants, Inc., 293 F.3d 707 (4th Cir. 2002) (discussing what is required to exercise personal jurisdiction over an out of state defendant who has directed electronic activity into the state).

test.[159] The ability of a court to exercise personal jurisdiction over a defendant depends on the construction of the state's long arm statute, on the case law in the individual jurisdiction, and depends heavily on the specific facts of the case.[160] Some plaintiffs will want to file in federal court based on diversity jurisdiction; depending on the jurisdiction, they may not be able to because there are John Doe defendants.[161]

Even if plaintiffs are able to win against defendants, the issue of damages provides a final hurdle to recovery. Because of ease of access, participation in Internet harassment is available for those who are effectively judgment proof, so "even where a plaintiff prevails in a civil action against an online harasser, the odds are high that the plaintiff will not be able to recover significant damages."[162] Without joint and several liability, each individual defendant is only liable for their comparative share of the damages, which is difficult to calculate when there may be thousands of possible defendants.[163]

C. Civil Conspiracy and its Features Adapted

In the twentieth century, tort law theories of liability grew significantly broader, at least partially as a way of encouraging socially beneficial behavior and punishing antisocial behavior.[164] Though this Note directly addresses only the tort of civil conspiracy, similar doctrines create liability for wrongful group action—either civil or criminal, ranging from civil Racketeer Influenced and Corrupt

---

159. Int'l Shoe Co. v. Wash., 326 U.S. 310 (1945) (holding that a defendant must have minimum contacts with a forum such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice). *See also* Allyson W. Haynes, *The Short Arm of the Law: Simplifying Personal Jurisdiction over Virtually Present Defendants,* 64 U. MIAMI L. REV. 133 (2009).

160. Haynes, *supra* note 159, at 160 (discussing the extensive amount of confusion and the lack of consistency in personal jurisdiction case law).

161. John Doe defendants are those that cannot be identified or that are allowed by the court to remain anonymous, and so John Doe is used as a placeholder. *See* Howell by Goerdt v. Trib. Entm't Co., 106 F.3d 215, 218 (7th Cir. 1997) ("But because the existence of diversity jurisdiction cannot be determined without knowledge of every defendant's place of citizenship, 'John Doe' defendants are not permitted in federal diversity suits."). Other courts hold that dismissal is premature until unmasking is achieved so that the plaintiff can name and serve the defendant. *See* Doe v. Ciolli, 611 F. Supp. 2d 216, 219-20 (D. Conn. 2009) (concluding that diversity jurisdiction for the purposes of unmasking is not defeated because of John Doe defendants, as the court can cure the jurisdictional issue by dismissing non-diverse parties subsequent to unmasking).

162. Kim, *supra* note 55, at 1008.

163. Restatement (Third) of Torts: Apportionment Liab. § 11 (2000).

164. Norman L. Greene, *Civil Conspiracy and the Rule of Law: A Proposal for Reappraisal and Reform*, 64 ARK. L. REV. 301, 308-09 (2011).

Organizations Act (RICO)[165] and anti-trust[166] to the inchoate crime of conspiracy[167]—to discourage wrongful group activity.[168] This Note proposes extending that logic to mass Internet harassment, using the tort of civil conspiracy as a way to discourage wrongful cybermob behavior and allow victims to recover damages.

In its simplest formulation, "[a] civil conspiracy is a group of two or more persons acting together to achieve an unlawful objective or to achieve a lawful objective by unlawful or criminal means."[169] Civil conspiracy cannot stand on its own as a cause of action, requiring some other illegal or tortious act before it can be asserted.[170] Because civil conspiracy is a common law cause of action, there can be substantial differences between different jurisdictions.[171] This Note uses the following definition of civil conspiracy: (1) two or more persons; (2) an unlawful objective or a lawful objective using unlawful means; (3) an agreement, understanding, or "meeting of the minds" regarding the objective and the means of pursuing it; (4) an unlawful act that is committed to further the agreement; (5) and harm; (6) that was proximately caused by the conspiracy.[172] These elements are, in large part, common to most jurisdictions and to most definitions of civil conspiracy.[173]

Two features of civil conspiracy make it a particularly effective tool to address the problem of cybermob harassment. First, civil conspiracy can be used as a "basis for establishing joint and several tort liability among several parties."[174] Each participant in the conspiracy is a joint tortfeasor, and therefore a court can order any member of the conspiracy to pay the full amount necessary to compensate a victim, regardless of how much harm the conspiracy member personally contributed.[175] Missing defendants and apportionment of damages is no longer an issue. Though some of the

---

165. 18 U.S.C.S. § 1964 (2017).

166. 15 U.S.C.S. § 1 (2017).

167. 18 U.S.C.S. § 371 (2017).

168. Both civil RICO and the Sherman Act create civil liability, which allows for the recovery of money damages.

169. Greene, *supra* note 164, at 301. This is a syncretic definition, as civil conspiracy is a common law tort.

170. Thomas J. Leach, *Civil Conspiracy: What's the Use?*, 54 U. MIAMI L. REV. 1, 2 (1999).

171. Greene, *supra* note 164, at 304.

172. 54 CAUSES OF ACTION 2d 603 (2012).

173. Greene, *supra* note 164, at 331-32; *see also* 16 Am. Jur. 2d Conspiracy § 50.

174. Leach, *supra* note 170, at 13.

175. *Joint-and-several-liability Doctrine*, BLACK'S LAW DICTIONARY (10th ed. 2014).

states do not include joint and several liability in their definition of civil conspiracy, for the purposes of this Note, the proposed civil conspiracy cause of action features joint and several liability.[176] Second, in some jurisdictions, civil conspiracy causes of action allow the extension of long-arm statutes.[177] The plaintiff's preferred court is then able to exert jurisdiction over a wider defendant pool because "the conspiracy itself [is] an *independent* source of jurisdiction over a nonresident defendant—regardless of the nonresident defendant's own contacts with the forum."[178] This Note treats this as a feature of its proposed civil conspiracy cause of action, even though some states do not extend jurisdiction as widely.[179]

The basis for the cause of action is agreement between conspirators; the logic underlying civil conspiracy is that organized group conduct is more dangerous than individual conduct.[180] The reason a conspiracy is more dangerous than individual action includes the notion that collective plans are less likely to be abandoned, and that "the strength, opportunities and resources of many is obviously more dangerous and more difficult to police than the efforts of a lone wrongdoer."[181] The agreement necessary for civil conspiracy does not have to be explicit; an implicit agreement is enough.[182] However, a person who not does know about the intent to injure or who assists in an unlawful act without knowing about the conspiracy is not liable.[183]

Where there is not an explicit agreement between conspirators, courts use a variety of factors in determining whether an implicit

---

176. *See* Greene, *supra* note 164, at 344-49 (discussing the limitations in joint and several liability in some state jurisdictions).

177. Leach, *supra* note 170, at 7 ("Some jurisdictions allow a plaintiff to use a conspiracy theory to support the court's exercise of long-arm jurisdiction over non-resident defendants, provided the court has personal jurisdiction over at least one conspirator.").

178. McKay Cunningham, *Attributing One Party's Contacts with the Forum State to Another: Conspiracy Jurisdiction in Alabama*, 71 ALA. LAW. 304, 307 (2010) (alteration in original).

179. *Id.* at 310 (discussing the differing views of states in regards to the extension of jurisdiction via the use of conspiracy).

180. *See generally* Neal Kumar Katyal, *Conspiracy Theory*, 112 YALE L.J. 1307, 1315 (2003); *see also* Greene, *supra* note 164, at 338 (noting this as a justification for civil conspiracy, even though disagreeing with that reasoning).

181. Krulewitch v. United States, 336 U.S. 440, 448-49 (1949) (Jackson, J., concurring).

182. 15A C.J.S. *Conspiracy* § 19 ("A party who understands the general objectives of the conspiratorial scheme, accepts them, and agrees (either explicitly or implicitly) to do its part to further those objectives is liable as a civil conspirator").

183. *Id.*

agreement exists.[184] "It is not necessary to prove an express agreement or compact among the wrongdoers; their common design may be inferred from the nature of the acts done, the relation between them, their mutual interests in the matter, and other circumstances."[185] "[I]t is enough that knowing concerted action was contemplated or invited, the defendant adhered to the scheme and participated in it."[186] The Restatement of Torts illustrates implicit agreement with two strangers in their vehicles who agree to race; the fact that a race resulted showed the agreement even though there was no explicit agreement between the two.[187]

An example from antitrust law illustrates how a party can commit similar acts while not being part of a conspiracy. In *Bell Atlantic Corp. v. Twombly,* the Court reiterated that a showing of parallel conduct alone was not sufficient to present a prima facie case of a conspiracy cause of action; the element of agreement was not met. In *Twombly*, the plaintiffs could not show an illicit act by the defendants, and each defendant acted in line "with a wide swath of rational and competitive business strategy unilaterally prompted by common perceptions of the market."[188] Because none of the defendants acted wrongly, and they all had rational reasons for the way they were acting, parallel behavior resulted even without explicit agreement. By merely identifying behavior that could have been the product of rational analysis without agreement, the plaintiffs were unable to show the agreement element of conspiracy.[189] To create a prima facie case for conspiracy, plaintiffs must additionally show that the problematic acts are not the result of parallel conduct but the result of a concerted agreement. The defendant is not liable when they lack knowledge of the object and purpose of the conspiracy, but those who

---

184. The element of agreement appears in a wide variety of conspiratorial contexts, from criminal to antitrust to copyright. This Note will use the tests for tacit agreement in a variety of different areas of law, differentiating when the areas of law are substantively different. This is appropriate because all of these areas of law are still focused on the key element to conspiracy—the agreement to act in concert. For a general overview of the various factors used to determine whether parties are acting in concert, implicitly or otherwise, see Restatement (Second) of Torts § 876 (1979).

185. Wright v. Apartment Inv. & Mgmt. Co., 726 S.E.2d 779, 787-88 (Ga. Ct. App. 2012).

186. Nicolet, Inc. v. Nutt, 525 A.2d 146, 148 (Del. 1987) (addressing conspiracy in regards to asbestos litigation).

187. Restatement (Second) of Torts § 876 (1979) (Comment on Clause (a): Illustration 2).

188. Bell Atl. Corp. v. Twombly, 550 U.S. 544, 545 (2007).

189. *Id.*

participate by planning, assisting, or encouraging a wrongdoer's acts are liable.[190]

II. THE PROBLEM OF CYBERMOBS AND CIVIL CONSPIRACY AS A REMEDY

This Note argues that the tort of civil conspiracy can be used to address cybermob harassment. The purpose is to give the victims of cybermob harassment a viable way to recover damages, even after accounting for all the difficulties of remedying Internet harassment. By providing both a method of recovery and a way to punish harmful behavior, civil conspiracy can discourage participation in cybermobs, while minimizing the chilling effect on lawful behavior.[191] This novel usage of civil conspiracy is warranted because of the extraordinary difficulties and challenges that victims, who have already had their lives upended, must overcome in order to get their day in court—not to mention actually recover the full extent of their damages.[192] Section II.A discusses the particular problem of cybermobs and how the aspects of the Internet discussed in Part I enable and facilitate cybermob harassment. Sections II.B and II.C addresses how the proposed civil conspiracy cause of action could be used to help plaintiffs unmask defendants and then bring them to court.

A. Cybermobs

The Internet allows those participating in cybermobs to "aggregate their efforts even when they have insufficient numbers in any one location to form a conventional hate group. [Members] can disaggregate their offline identities from their online presence, escaping social opprobrium and legal liability for destructive acts."[193] Social networking sites, chatrooms, and forums allow members of destructive groups to deliberate, creating an echo chamber that reinforces preexisting views and encourages the growth of extremism.[194] In combination with anonymity, this effect polarizes group members,[195] and causes members to lose a sense of

---

190. *See* 15A C.J.S., *supra* note 182.

191. The author of this Note does not argue that this novel approach is the ideal, best solution. The author acknowledges that the best way to address cybermobs in general may be to change the CDA, but has misgivings because of the mass nature of cybermob harassment.

192. *See*, *e.g.,* Kim, *supra* note 55, at 1008-12 (discussing the various inadequacies of existing remedies).

193. Citron, *supra* note 74, at 63.

194. *Id.* at 81.

195. CITRON, *supra* note 19, at 63.

responsibility for their destructive acts.[196] Social media mainstreams destructive group behavior through mob shaming, which then creates a larger audience for cybermobs and a larger potential pool of cybermob participants.[197]

Legal scholars address cybermobs less often than cyberstalking or cyberbullying.[198] However, social commentators and other media address the phenomenon of cybermobs extensively,[199] especially in light of the number of large-scale cybermob campaigns in the last five years.[200] Cybermobs consist of: (1) a group of persons acting in cyberspace, (2) joining together to harass (3) a victim or victims, (4) for a real or imagined misdeed or faux pas.[201] The commentary on cybermobs focuses on the key element, mass action by large numbers of anonymous Internet users, acting in concert to punish the target as a reaction to a trigger.[202] A trigger event happens and then a collective hive mind forms, aggregating individual actions and causing harm, even if individual members have not explicitly agreed to target a given victim.[203] Within cybermobs can be factions that are

---

196. *Id.*

197. *See, e.g.,* Fisher, *supra* note 11. Social media allows the quick dissemination of outrage, compounding the issues mentioned in Part I. This in turn creates a larger audience for cybermob participants, which then can compound into an "information cascade" that reinforces the persistence of any harmful speech.

198. Professor Citron is the most prolific writer in the legal literature in regards to cybermobs explicitly. Other scholars address cybermobs in passing or as an outgrowth of other phenomenon and not as their own unique social ill.

199. *See*, *e.g.,* Nick Bilton, *When the Cyberbully Is You*, N.Y. TIMES (Apr. 29, 2015), http://www.nytimes.com/2015/04/30/style/when-the-cyberbully-is-you.html [https://perma.cc/Q2FC-NL48].

200. These include GamerGate, Cecil the Lion, Justine Sacco, and Sunil Tripathi, among others. This Note recognizes that at least some of these campaigns have mob shaming elements that do not involve cybermob harassment. This Note separates the two, based on wrongfulness of behavior, recognizing that the two groups intermingle and that wrongfulness can be blurred. At the same time, there is a qualitative difference between someone sharing news articles about Cecil the Lion and someone calling in death threats to Walter Palmer. If this author continues to write about this subject, he believes it would be interesting to try and delineate trolling, online shaming, and cybermobs in a more concrete manner. *See* Fisher, *supra* note 11.

201. This definition appears in UrbanDictionary.com, a wiki for slang terms. *Cybermob*, URB. DICTIONARY (Feb. 24, 2008), http://www.urbandictionary.com/define.php?term=cybermob [https://perma.cc/QFL8-7FGE]. The discussion about cybermobs includes these features, even though they do not necessarily define these elements precisely. *See* CITRON, *supra* note 19, at 5; Fisher, *supra* note 11; Ronson, *supra* note 15.

202. Fisher, *supra* note 11.

203. *Id.*

themselves smaller cybermobs. Some of these factions are explicit, organized groups that agree to attack a given target.[204]

Cybermobs form around a real or imagined misdeed or faux pas.[205] From killing a beloved animal,[206] to blogging about feminist issues,[207] there is some reason that the targeted victim becomes the focus of cybermob harassment. These reasons can be false, such as due to misidentification, or can be the result of legitimately deplorable actions.[208] Some members of cybermobs see themselves not as harassers, but as cyber-avengers, punishing perceived wrongdoers.[209] Some of the victims are not particularly sympathetic human beings.[210] Some are completely innocent people who have, through no fault of their own, drawn the ire of a cybermob.[211] In any case, what unites them is that they are specifically targeted for mass harassment because some event brought them to prominence. Cybermob

---

204. For example, an Anonymous offshoot, KY Anonymous, targeted Hunter Moore, the proprietor of "Is Anyone Up?" which is a famous and now defunct revenge porn site. CITRON, *supra* note 19, at 54-55. Anonymous is a cyber collective of activists and hackers. For a more in-depth discussion of anonymous, see David Kushner, *The Masked Avengers*, NEW YORKER (Sept. 8, 2014), http://www.newyorker.com/magazine/2014/09/08/masked-avengers [https://perma.cc/N3AF-QXH4].

205. For example, the Cecil the Lion campaign formed after Walter Palmer killed the eponymous lion. GamerGate was actually comprised of multiple campaigns that conglomerated; the campaign that targeted Zoe Quinn started because an ex-boyfriend accused her of trading sexual favors for press coverage, while the GamerGate campaign targeting Anita Sarkeesian resulted from the release of the newest episode of "Tropes vs. Women in Video Games," a YouTube series deconstructing sexist tropes in video games. Cybermobs targeted her upon the release of the original videos, but renewed their assault as part of the GamerGate campaign because an episode release coincided with the accusations against Zoe Quinn.

206. *See* Fisher, *supra* note 11.

207. *Id.*

208. Sunil Tripathi's family received a series of threatening phone calls after Reddit falsely identified him as the Boston Bomber, while the KY Anonymous campaign came about as a result of Hunter Moore featuring the wrong person on his revenge porn site. *Compare* Kang, *supra* note 4, *with* CITRON, *supra* note 19, at 54-55.

209. Ronson, *supra* note 15 ("[T]he collective fury felt righteous, powerful and effective. It felt as if hierarchies were being dismantled, as if justice were being democratized.").

210. Hunter Moore is an obvious example. But Anonymous targets far more deplorable people as well including supposed members of the KKK and ISIS. *See Anonymous Posts Ku Ku Klan Alleged Sympathizers List*, BBC TECH. BLOG (Nov. 6, 2015), http://www.bbc.com/news/technology-34736941 [https://perma.cc/GL2T-MR44]; Katie Rogers, *Anonymous Hackers Fight ISIS but Reactions Are Mixed*, N.Y. TIMES (Nov. 25, 2015), http://www.nytimes.com/2015/11/26/world/europe/anonymous-hackers-fight-isis-but-reactions-are-mixed.html [https://perma.cc/QX29-RZ93].

211. *See, e.g.,* Kang, *supra* note 4.

harassment is about mass action and virality; its ability to harm is an outgrowth of many actors committing relatively minor acts that culminate into a course of conduct, rather than an individual actor dedicated to harming a given target.[212] Publicity and group participation are the core components of cybermob harassment.[213] The echo chamber effect created by the Internet's easy group formation takes place in public, with a mainstream audience watching.[214]

The cybermob commentary from popular media conflates both legitimate speech and tortious activity in its concern about the social phenomenon of mass cyber shaming.[215] This Note separates the campaigns based on the tactics used. While acknowledging that the harm can also be caused by First Amendment-protected speech and that First Amendment-protected speech can be used as part of the larger cybermob campaign, this Note focuses on tortious activity and non-protected speech.[216]

B. Civil Conspiracy, Copyright Law, and Permissive Joinder

Cybermobs cause harm through mass action, which makes the process of individually litigating against each possible defendant an extraordinarily expensive proposition. Copyright law deals with the same problem of unmasking what could be thousands of defendants.[217] Courts are split on whether permissive joinder—providing a basis for mass unmasking—should be allowed in those cases out of fear of abuse.[218] Courts are afraid that plaintiffs will use joinder and unmasking as a way of either intimidating or blackmailing

---

212. *See* Fisher, *supra* note 11.

213. *See, e.g.,* CITRON, *supra* note 19, at 5 ("Online harassment can quickly become a team sport, with posters trying to outdo each other. Posters compete to be the most offensive, the most abusive."); Fisher, *supra* note 11 ("It is not primarily about punishing the crime or the criminal, but rather about indulging the outrage of the mob and its thirst for vengeance.").

214. CITRON, *supra* note 19, at 63.

215. *See supra* notes 4-11.

216. For example, calling Justine Sacco a horrible person and a racist would be protected speech, as it is an opinion. This could cause harm, as it would turn up in a background check. But it would not be actionable harm. *See* Ronson, *supra* note 15.

217. *See* Donkeyball Movie, LLC v. Does, 810 F. Supp. 2d 20, 29-31 (D.D.C. 2011) (discussing the balance courts must strike between the rights of copyright holders and the possible strains on judicial economy in considering whether to sever hundreds of defendants in mass copyright infringement cases). Many of these copyright cases involve file-sharing, which means there could be many thousands of defendants infringing by downloading and hosting copyrighted files.

218. *See* Larson & Godfread, *supra* note 144, at 343-47 (discussing the types of process abuse present in mass unmasking actions).

defendants; other courts are afraid of the possible chilling effect on speech if unmasking is too permissive.[219] These copyright cases deal with intellectual property claims rather than the personal torts alleged in cybermob harassment, but there are some similarities. Some of the reasons that joinder is granted in copyright cases apply also to cybermob cases; most of the reasons why courts do not grant joinder are distinguishable, while others are potential problems in cybermob litigation.

Courts that allow joinder in mass copyright cases usually ground their analyses on the protection of the copyright holder's rights. Copyright holders have rights that anonymous defendants allegedly infringed, and because of the nature of the Internet, there is no other feasible way to protect those rights.[220] If joinder is not granted, plaintiffs would need to file separate lawsuits and move to issue separate subpoenas and pay separate filing fees, forcing plaintiffs to "face significant obstacles in their efforts to protect their copyrights from illegal file-sharers and this would only needlessly delay their cases."[221] Cybermob plaintiffs similarly have the legal right to protect themselves from harassment and tortious harm, but civil litigation is currently not a feasible way of protecting those rights.[222] Cybermob plaintiffs similarly face the problem of filing expensive individual lawsuits against many defendants.[223] Though some copyright defendants claim that joinder and unmasking violates First Amendment protections, the First Amendment does not protect

---

219. *Id.*; *see also* Violeta Solonova Foreman, Note, *Problems with Bittorrent Litigation in the United States: Personal Jurisdiction, Joinder, Evidentiary Issues, and Why the Dutch Have a Better System*, 13 WASH. U. GLOBAL STUD. L. REV. 127 (2014).

220. *See*, *e.g.*, *Donkeyball*, 810 F. Supp. 2d at 30 ("[C]opyright owners have limited alternatives to obtain redress for infringement of their protected works other than such lawsuits."); Arista Records LLC v. Does 1-27, 584 F. Supp. 2d 240, 252 (D. Me. 2008) ("Under the law, the Plaintiffs are entitled to protect their copyrighted material and it is difficult to discern how else in this unique circumstance the Plaintiffs could act.").

221. Call of the Wild Movie, LLC v. Does 1-1,062, 770 F. Supp. 2d 332, 344 (D.D.C. 2011).

222. *See generally supra* Part I.

223. It costs $350 to file a civil action in federal district court. *See* 28 U.S.C.S. § 1914(a) (2017) (listing district court filing fees). Without joinder, a plaintiff would have to file an individual claim against each defendant. Cybermob plaintiffs, by dint of being the alleged victims of cybermobs, will inevitably have to deal with many defendants. *See* discussion *supra* Part I.

copyright infringement.[224] Similarly, the First Amendment does not protect tortious speech.[225]

Courts deny joinder for a variety of reasons, many of which are distinguishable in cybermob harassment cases. Some courts find that the connection between defendants is too attenuated to establish a single transaction or occurrence.[226] The courts rely on how the infrastructure of Internet file-sharing technology makes it difficult to discern a connection between the putative defendants, other than the use of a similar technology.[227] However, this reasoning is based on a very narrow reading of transaction or occurrence, while the facts of cybermob harassment and its nexus of time, trigger, and concerted action distinguish cybermob harassment from file-sharing.[228]

Other reasons for denying joinder in copyright infringement cases do, however, apply to cybermob harassment cases. Misidentification is a possibility, as there is no guarantee that an IP address actually belongs to a specific mob participant.[229] Other courts identify the problem of abuse, of plaintiffs using unmasking to either extort settlement payments from putative defendants or to chill criticism.[230] However, these problems are seemingly inherent in Internet litigation with large numbers of anonymous defendants.[231] There is no real alternative for plaintiffs, and so it should fall to the courts to prevent these abuses by exerting courts' power to manage both joinder and discovery more generally.

There is some precedent for the extension of the civil conspiracy cause of action into cyberspace in order to join defendants.

---

224. Arista Records, LLC v. Doe 3, 604 F.3d 110, 118 (2d Cir. 2010).

225. *See* David L. Hudson, Jr., *Libel & Defamation*, FIRST AMEND. CTR. (Sept. 13, 2002), http://www.firstamendmentcenter.org/libel-defamation [https://perma.cc/TV5D-2EXT] (describing the tension between defamation/libel law and the First Amendment).

226. *See* Digital Sins, Inc. v. John Does 1-245, No. 11 CIV. 8170 CM, 2012 WL 1744838, at *2 (S.D.N.Y. May 15, 2012) ("[P]laintiff [in Bittorrent copyright infringement suit] does no more than assert that the defendants 'merely commit[ed] the same type of violation in the same way,' it does not satisfy the test for permissive joinder in a single lawsuit pursuant to Rule 20.").

227. *See* Kristina Unanyan, Note, *Walk A Mile in the Shoes of a Copyright Troll: Analyzing and Overcoming the Joinder Issue in Bittorrent Lawsuits*, 8 J. BUS. ENTREPRENEURSHIP & L. 629, 641-42 (2015); *see also* Larson & Godfread, *supra* note 144, at 344-45.

228. *See* discussion *infra* Section II.C.

229. *See* Digital Sins, Inc. v. Does 1-176, 279 F.R.D. 239, 242 (S.D.N.Y. 2012) (discussing the likelihood, thirty percent in that case, that the IP addresses actually belong to a third party using the putative defendants' Internet access).

230. *See* Larson & Godfread, *supra* note 144, at 344-47.

231. *See* discussion *supra* Part I.

Copyright holders have used civil conspiracy as support for joinder.[232] A civil conspiracy cause of action could strengthen a plaintiff's arguments for joinder, as there would be a common question of law: whether the tortious acts alleged were part of a civil conspiracy.[233] Most courts deny civil conspiracy claims in copyright file-sharing cases, reasoning that either federal copyright claims preempt the state law civil conspiracy claims, as both types of claims protect the same rights, or that plaintiffs cannot establish the agreement necessary.[234] Cybermob harassment is distinguishable firstly because there is no federal preemption and, secondly, because agreement is easier to show in cybermob harassment cases.[235]

C. Civil Conspiracy and Cybermobs

The proposed civil conspiracy cause of action could ease many of the challenges plaintiffs face in Internet harassment cases, especially those dealing with cybermobs. The purpose of exploring this novel cause of action is to fill a current gap in the law created by CDA section 230(c).[236] Victims are harmed by cybermobs, but cannot recover.[237] Cybermob participants learn that there are no consequences for harassing others on the Internet.[238] By allowing plaintiffs to more easily recover Internet harassment damages, courts can discourage participation in cybermobs.

The proposed civil conspiracy cause of action would cure two core issues in civil litigation of cybermob Internet harassment.[239] First, civil conspiracy could help plaintiffs meet the unmasking standards by providing grounds for joinder, and providing a cause of action around which to build an unmasking analysis. Meeting the elements of a civil

---

232. Sunlust Pictures, LLC v. Does 1-75, No. 12 C 1546, 2012 WL 3717768, at *4 (N.D. Ill. Aug. 27, 2012) ("Sunlust's civil conspiracy claim further supports joinder. Sunlust alleges that Doe and the other defendants entered into a conspiracy to unlawfully distribute the Video by joining a single Bittorrent swarm.").

233. *Id.*; *see also* First Time Videos, LLC v. Does 1-76, 276 F.R.D. 254, 257-58 (N.D. Ill. 2011) (holding that whether participation in a torrent swarm constitutes a civil conspiracy is a question of law sufficient to justify joinder).

234. *See* Hard Drive Prods., Inc. v. Does 1-188, 809 F. Supp. 2d 1150, 1163 (N.D. Cal. 2011) (describing why agreement cannot be established in cases involving the Bittorrent protocol); *see also* Two Palms Software, Inc. v. Worldwide Freight Mgmt., LLC, 780 F. Supp. 2d 916, 921-22 (E.D. Mo. 2011) (holding that a federal copyright claim precluded a common law civil conspiracy claim). Though *Two Palms* does not involve file-sharing per se, it does consider similar Copyright Act claims.

235. *See* discussion *infra* Section II.C.

236. *See* discussion *supra* Section I.B.

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

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

239. *See* discussion *supra* Section I.B.

conspiracy would allow an unmasking subpoena to survive either a prima facie test or summary judgment test.[240] By making it easier to unmask, plaintiffs would have a larger pool of possible defendants.[241] This is a necessary feature for civil litigation, as plaintiffs in cybermob harassment cases will inevitably be unable to find or establish jurisdiction over some potential defendants.[242] Secondly, civil conspiracy liability could provide a way to establish jurisdiction through extending long-arm statutes.[243] Civil conspiracy's joint and several liability would make it easier for plaintiffs to recover the full amount of their damages. With a larger pool of viable defendants and joint and several liability, there is a greater likelihood that there will be an accessible defendant with resources capable of making the plaintiff whole.

The features of cybermob harassment satisfy the elements of civil conspiracy.[244] Cybermobs are groups of people, who become associated by targeting a specific victim due to a specific event.[245] Cybermob participants act in concert, with the knowledge that others are acting similarly, and they act with similar objectives.[246] Internet harassment is an unlawful objective.[247] Even if the stated objective, such as expressing displeasure with a victim's actions, is judged lawful, harassment tactics like libel are unlawful means by which the lawful objective is pursued. The harassment tactics provide the unlawful basis for the civil conspiracy cause of action. Harm from a cybermob is proximately caused by the agreement of the participants.

The most important element of civil conspiracy, agreement, can be established most easily in instances where there is explicit agreement between cybermob participants, such as with groups like Anonymous.[248] Agreement can also be established where there is no

---

240. *See* discussion *supra* Section I.B.

241. *See* discussion *supra* Section I.B. Without unmasking, there may be no defendants, as there would be no one to sue unless the tortious posting was done under the alleged tortfeasor's real name, and there were no issues of identification.

242. *See* discussion *supra* Section I.B.

243. *See* discussion *supra* Section I.B.

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

245. *See* discussion *supra* Section II.A.

246. *See* discussion *supra* Section II.A.

247. *See* discussion *supra* Section I.A.

248. *See, e.g.,* Emily Bazelon, *The Online Avengers*, N.Y. TIMES MAG. (Jan. 15, 2014), http://www.nytimes.com/2014/01/19/magazine/the-online-avengers.html [https://perma.cc/BE79-LJCR] ("None of the OpAntiBully members ever met in person, but they began spending hours working together online, using encrypted email accounts or chat rooms for anything they deemed sensitive."). Though these

explicit agreement because of the resulting campaign of harassment.[249] The conspirators have a common goal, to harass or punish the victim; there is no rational reason for them to each act separately when attacking their victim.[250] There is a common nucleus of events that precipitate the campaign. The same events motivate the conspirators to attack the victim.[251] Participants know or should know that others are acting similarly, that the actionable tactics they use are illegal, and yet agree that the target should be punished.[252] Time and a triggering event tie the cybermob participants together; this nexus makes it unlikely that they chose the victim at random, with no consideration of agreement.

This does not mean that civil conspiracy liability adheres to each and every person who expresses their displeasure against a given target for a given reason. After all, the person who firebombs a polluting factory is fundamentally different than the person who pickets in front of that same factory; they both share the same ultimate purpose of ending the factory's polluting ways, but their short term objectives and their methods are vastly different. This Note proposes that each named defendant must commit an affirmative act that is either tortious or that directly facilitates the conspiracy. This would include the doxxer,[253] the person planning campaigns in support of wrongful tactics, and those who have actually committed allegedly tortious actions. This limitation is in keeping with the various unmasking tests. The *Cahill*,[254] *Dendrite*,[255] and *Mobilisia*[256] tests all require that plaintiffs set out the exact actionable posts or items upon which the plaintiffs will build their case.[257] To sustain a civil conspiracy cause of action against a defendant, a plaintiff needs to show the court the exact posts or actions that would

---

Anonymous members used some positive tactics, such as encouragement to bullying victims, they also worked together to doxx and attack those identified as bullies.

249. *See* discussion *supra* Section I.C.

250. *Compare supra* notes 5, 6, 9, 11 (for examples of how perfect strangers came to attack individual victims in parallel for no rational purpose), *with supra* notes 188-90 (showing parallel action without agreement due to shared rational reasoning). To a large extent, that's what makes cyber shaming and cybermob harassment so terrifying. These are people who have no connection to the victim except their shared desire to harm them.

251. *See* discussion *supra* Section II.A.

252. *See* discussion *supra* Section I.C.

253. *See* Dewey, *supra* note 24.

254. *See supra* notes 150-53.

255. *See supra* notes 145-49.

256. *See supra* note 153.

257. *See* discussion *supra* Section I.B.2.

indicate membership in the conspiracy.[258] If plaintiffs seek to unmask only those who the plaintiff can show took affirmative action in furtherance of the conspiracy, the plaintiff should succeed in getting an unmasking subpoena. Because of joint and several liability, plaintiffs can still hold any single defendant responsible for all the harm from the conspiracy, which prevents the plaintiff from having the missing defendant problem.

These mechanisms can help avoid or minimize the issues and problems discussed earlier regarding Internet litigation and civil conspiracy.[259] By limiting those included in the conspiracy in this manner, the problem of over-inclusion is mitigated,[260] and the possible chilling effect on speech minimized. Overly expansive criteria for membership in the conspiracy could lead to the relatively blameless being responsible for the plaintiff's damages.[261] Over-inclusion and unmasking can both lead to chilling of speech, as Internet users self-censor in order to avoid punishment.[262] This also addresses concerns in file-sharing cases by hedging against misidentification and meritless abuse; the court can decide whether a given post linked to a given IP address is actionable.[263]

The purpose of using civil conspiracy in a cybermob case is not to spread liability beyond those who are wrongdoers. Public shaming can cause real harm, but is not in and of itself actionable without a wrongful act.[264] This Note specifically addresses civil conspiracy

---

258. *See* discussion *supra* Section I.B.2. While the good cause test does not require delineation of the exact actionable material, the more common *Dendrite* and prima facie cases do.

259. *See* discussion *supra* Part I.

260. Because of how people connect to the Internet, there will inevitably be some misidentification, as IP traces are inexact. In file-sharing cases, some defendants were not the ones actually participating in the file-sharing networks, but rather those whose Internet had been misappropriated in some way. However, the courts can protect against misidentification. *See, e.g.,* Digital Sins, Inc. v. Does 1-176, 279 F.R.D. 239, 242-43 (S.D.N.Y. 2012). In that case, a John Doe defendant claimed that they were not liable because they did not know how to use a computer. The court ordered a temporary protective order to allow defendants to respond to the subpoena to defend against extortion attempts by the plaintiff.

261. For example, an overly expansive view of conspiracy could mean that those who applaud or encourage cybermob action without actually either participating by committing a tortious act or helping to facilitate such an act by doing something like doxxing would be included in the conspiracy. Encouragement of cybermob behavior may be reprehensible, but such encouragement is not tortious.

262. *See* discussion *supra* Section I.B.2.

263. *See supra* notes 257-58.

264. *See* Ronson, *supra* note 15. Some of the abuse Justine Sacco received was wrongful, such as threats. However, most of the harm she suffered originated from

because the commission of an illicit act is a central element. Public shaming—such as notifying employers of racists posts by employees, or making fun of people's opinions—is not the issue addressed herein.[265] Truth can be harmful, but it is not actionable. Mass public shaming may be a social ill that should be addressed, but it is explicitly not within the purview of this Note. Instead, this Note keeps itself firmly grounded in the goal of recovering for illicit actions because there is a difference between stating that someone is a racist and saying that they have herpes, or that they are criminals.[266]

III. AUTOADMIT AND CIVIL CONSPIRACY IN PRACTICE[267]

Part III examines one litigated example of cybermob harassment. Examining the facts of the case, this Part argues that the elements of civil conspiracy are present, and uses this as a basis upon which other examples of cybermob harassment similarly fit the traditional elements of civil conspiracy.[268] It further addresses possible problems and inadequacies that could arise from using civil conspiracy to combat cybermob harassment.

One of the first cases to address cybermob-style harassment is *Doe I v. Individuals* ("*AutoAdmit*").[269] The plaintiffs did not allege civil conspiracy as a cause of action, but the facts of the case would be sufficient to meet this Note's proposed civil conspiracy elements. However, *AutoAdmit* is still a useful case to consider because it is one of the few cases that discuss cybermob-style harassment and unmasking.

AutoAdmit.com is an Internet forum with thousands of users who affirmatively participate in the community by registering, and by

---

the shaming she received for the racist joke she tweeted. This Note tries to draw the balance between protected shaming and unprotected harassment.

265. *See, e.g.*, Ronson, *supra* note 15.

266. *See, e.g.*, Complaint, Doe I v. Individuals, 561 F. Supp. 2d 249 (D. Conn. 2008) (No. 307CV00909 CFD).

267. This Part uses the facts from *AutoAdmit*. Doe I v. Individuals, 561 F. Supp. 2d 249 (D. Conn. 2008). This Note assumes the plaintiffs' allegations are true. It does so because a court would need to view the facts in the light most favorable to the non-moving party in a summary judgment motion. Because plaintiffs need to survive a summary judgment test in order to unmask and thereby have their day in the court, treating the allegations as true is appropriate.

268. *See* discussion *supra* Section I.C (discussing elements of civil conspiracy).

269. *AutoAdmit*, 561 F. Supp. 2d 249. It is also the most discussed case, because it has been extensively covered in both the regular media as well as scholarship. This is likely due to it being one of the few cases discussing the logic of Internet harassment and unmasking.

posting on the forum.[270] There are likely many more users that browse AutoAdmit, reading threads without choosing to participate in the discussions.[271] The plaintiffs, Jane Doe I and Jane Doe II, alleged libel, invasion of privacy, negligent and intentional infliction of emotional distress, and copyright violations committed by AutoAdmit posters starting in 2005 for Doe I and 2007 for Doe II.[272] The suit stemmed from a series of postings on the AutoAdmit website, including statements "that [Doe II] fantasized about being raped by her father, that she enjoyed having sex while family members watched, that she encouraged others to punch her in the stomach while seven months pregnant, that she had a sexually transmitted disease, [and] that she had abused heroin."[273] Some of the posters revealed personal information indicating that they were Doe II's classmates at Yale Law School and were in personal contact with her.[274] The harassing course of conduct was not restricted to merely posting on the forum, but quickly crossed over into other spaces.[275] A poster sent an email to a member of the Yale Law School faculty about Doe II and her father's alleged criminal history.[276] Another poster claimed that they sent an email to one of Doe II's future employers, recounting the claims made in the AutoAdmit threads.[277] The plaintiffs tried to serve notice on thirty-nine AutoAdmit posters who allegedly committed affirmative tortious acts.[278] The plaintiffs sued in federal court because of a copyright claim, and also brought state law tort claims via supplemental jurisdiction.[279]

The *AutoAdmit* defendants fit the requirements to be a cybermob.[280] There were thirty-nine posters subpoenaed in *AutoAdmit*, all of whom were members of the forum.[281] They joined

---

270. *See AutoAdmit*, AUTOADMIT, https://www.autoadmit.com [https://perma.cc/62TZ-MWCD].

271. AutoAdmit.com is open to users who are not registered. They may view posts but cannot start threads, reply to topics, or send private messages to other viewers. *See id.*

272. *AutoAdmit*, 561 F. Supp. 2d at 251.

273. *Id.*

274. *Id.*

275. *See* Complaint, Doe I v. Individuals, 561 F. Supp. 2d 249 (D. Conn. 2008) (No. 307 CV 00909 CFD).

276. *AutoAdmit*, 561 F. Supp. 2d at 251.

277. *Id.*

278. CITRON, *supra* note 19, at 133.

279. *AutoAdmit*, 561 F. Supp. 2d at 253.

280. *See* discussion *supra* Section II.A.

281. *See AutoAdmit*, 561 F. Supp. 2d at 251.

together to harass the two Jane Does. Their coordination is evident via their posts, where they made the comments public and bragged about what they were doing.[282] The defendants acted to harass the plaintiffs in retaliation for the plaintiffs' attempts to remove the plaintiffs' photos from the AutoAdmit website.[283] Though there were no faux pas committed by the two plaintiffs, the initial threads that brought the plaintiffs to AutoAdmit's attention and designated them as targets acted as the triggering impetus for the subsequent wrongs.

A. Civil Conspiracy Elements Present

The elements of a civil conspiracy are: (1) two or more persons; (2) an unlawful objective or a lawful objective using unlawful means; (3) an agreement, understanding, or "meeting of the minds" regarding the objective and the means of pursuing it; (4) an unlawful act that is committed to further the agreement; (5) and harm; (6) that was proximately caused by the conspiracy.[284] The following Section discusses how the *AutoAdmit* case is exemplary of a civil conspiracy case that could serve as a model for litigation involving cybermob harassment.

1. Group of Two or More

This element is satisfied because there were thirty-nine different users that were named in the suit and who were subpoenaed.[285] Even assuming that some of the usernames were sock-puppets,[286] the

---

282. *Id.* The following exchange is an example of how the posters played off each other:

> [Poster I]: 'I can assure you she doesn't dress conservatively. Anyone who goes to the gym in the afternoon has seen her trapsing [sic] around in spandex booty shorts and a strappy tank top. She wants people to look, and they do.' . . . [Poster II]: 'Take your goddamned cell phone next time and snap a pic, for Chrissakes. Then post, oc.' This invitation to stalk Doe II appears on a thread entitled "Huge Fucking Titties at Yale Law School (YLS). . . .

Complaint at ¶ 43, Doe I v. Individuals, 561 F. Supp. 2d 249 (D. Conn. 2008) (No. 307CV00909 CFD).

283. *See* Complaint, *AutoAdmit,* 561 F. Supp. 2d 249.

284. *See* discussion *supra* Section I.C.

285. *See AutoAdmit*, 561 F. Supp. 2d 249.

286. Sockpuppeting is the creation and manipulation of online identities for the purpose of deception. For example, a CEO who sees posts about themselves on a forum decides to create a profile, ostensibly of a neutral customer, to defend themselves under the false identity. *See* Brad Stone & Matt Richtel, *The Hand That Controls the Sock Puppet Could Get Slapped*, N.Y. TIMES (July 16, 2007), http://www.nytimes.com/2007/07/16/technology/16blog.html [https://perma.cc/6582-3285].

plaintiffs' subpoenas revealed at least seven different defendants.[287] The number of *AutoAdmit* defendants meets the number element of civil conspiracy.

More generally in cybermob cases, the number of possible defendants will likely be the easiest element to satisfy because of the mass nature of cybermob campaigns. There may be issues with sockpuppeting and other tactics that multiply one user's web presence.[288] But, if after the unmasking process, a plaintiff discovers that all of their harassment originates with one IP address or one user, the plaintiff can amend their complaint.

2. Unlawful Objective/Lawful Objective by Unlawful Means

The *AutoAdmit* defendants could claim that they had a lawful objective, such as poking fun at the plaintiffs in a harmless manner. Even if the objective is lawful, the plaintiffs alleged unlawful acts that would still meet the element of unlawful means.[289] This analysis is the best way to understand cybermob goals in general. Cybermob harassment campaigns are about hurting a target for a given reason, which should be an unlawful goal.[290] This does run up against the problem of public shaming, which is protected under the First Amendment. In the Justine Sacco and Cecil the Lion campaigns, there was both lawful and unlawful public punishment of the targets.[291] However, the difference between lawful and unlawful attempts lies in the tactics employed. It is protected speech to call someone a horrible person; it is not protected to accuse them of being a child molester or to threaten their life.[292] These means lead into the common agreement between conspirators, as it is the choice of tactics used that binds the participants in a cybermob together.

3. Agreement

Those affirmatively participating in the tortious acts were part of an agreement, implicit though it may have been, to cooperate and to harass. Some of the posters that were subpoenaed actively posted defamatory material on the website and elsewhere.[293] Others chose to take the campaign into the physical world by allegedly calling the

---

287. CITRON, *supra* note 19, at 133.

288. *See* Stone & Richtel, *supra* note 286.

289. *See* Complaint, Doe I v. Individuals, 561 F. Supp. 2d 249 (D. Conn. 2008) (No. 307CV00909 CFD).

290. *See* discussion *supra* Section II.A.

291. *See* Ronson, *supra* note 15; Fisher, *supra* note 11.

292. *See* Hudson, *supra* note 225.

293. *See* Complaint, *AutoAdmit,* 561 F. Supp. 2d 249.

plaintiffs' employers and spreading libel.[294] Libel and defamation are tortious acts unprotected by the First Amendment.[295] Posters shared their exploits in a forum together; they targeted the plaintiffs because other AutoAdmit users posted about the defendants; the defendants knew that other posters also acted against the plaintiffs.[296] The alleged acts were tortious in nature, defamatory untruths, and threats.[297] The relation between the defendants was in their membership in the AutoAdmit forum, where they egged one another on and bragged about their attacks against the plaintiffs.[298] The defendants' only mutual interest in the matter was their membership in the forum and their desire to harm or harass the plaintiffs.[299] The first tortious posting could be inferred as an invitation for concerted action, as others jumped in and participated in the scheme. None of the *Twombly* factors would support the argument that these were individual, rational actions.[300] None of the defendants had anything to gain by their participation.[301]

This is likely to be difficult to establish in every cybermob case. There was a record of the AutoAdmit defendants participating in a thread together.[302] However, some sites on which cybermobs organize, such as 4chan, do not keep logs.[303] It would be difficult to identify which poster did what, especially because sites like 4chan anonymize their users.[304] The plaintiffs' selection of *AutoAdmit* defendants was a good example of how to limit the number of defendants. The *AutoAdmit* plaintiffs subpoenaed all those who had posted allegedly tortious material.[305] The plaintiffs chose not to sue everyone who posted in the thread itself, likely because not everyone

---

294. *Id.*

295. *See* Hudson, *supra* note 225.

296. *See* discussion *supra* Section II.C.

297. *See* Complaint, *AutoAdmit,* 561 F. Supp. 2d 249.

298. *Id.*

299. *AutoAdmit*, 561 F. Supp. 2d at 251-52.

300. *See supra* notes 188-90.

301. This is inferred, as participation on AutoAdmit does not provide any material benefit, nor any reputational benefit, as usernames are not tied to a person's real identity. While there may be gain from reading some of the postings, for example if the postings gave advice, there was nothing beneficial about posting in the threads about the plaintiffs.

302. *See* Complaint, *AutoAdmit,* 561 F. Supp. 2d 249.

303. *See* 4CHAN, *supra* note 8. 4chan "prunes" threads that go beyond a certain number of pages for each of its individual boards. Once the system is pruned, it is irretrievable except insofar as someone chooses to save copies of the thread somewhere else.

304. *See supra* note 118 and accompanying text.

305. *See* Complaint, *AutoAdmit,* 561 F. Supp. 2d 249.

in the thread took affirmative action to post tortious material or to commit tortious acts. In other cases, it will be similarly difficult to establish an agreement. It will only be easy when it is a distinct group that is explicitly trying to attack a target, such as when a plaintiff has chat logs or forum posts identifying harassers.[306] Otherwise, the impromptu cybermobs that form in places like 4chan are not documented unless a user chooses to screenshot forum posts, because 4chan does not archive its threads.[307] Though chat logs explicitly discussing agreement would be the best way to show the existence of a conspiracy and membership by at least some members, the implicit agreement theory discussed above could also work in other cybermob cases.[308]

Plaintiffs should be able to show agreement however, by presenting the nexus of time, trigger, and collective action. Cybermob participants do not individually and coincidentally choose the same target; they attack because of a trigger.[309] The campaigns begin after the trigger, rise to a crescendo of maximal participation, and then die down. Harassment outside of that nexus may be too attenuated, but harassment within that nexus should be sufficient to show concerted action. Because there is no rational reason for individual users to act in a tortious manner, the defendants acted wrongly, and because of their awareness of each other's activities, there is no problem of parallel action.[310] For example, the cybermob harassment of Sunil Tripathi's family began when he was misidentified as the Boston Marathon Bomber.[311] The harassment that arose in the immediate aftermath of that misidentification would be within that nexus, but actions after the misidentification became common news would not

---

306. *See, e.g.,* Greg Tito, *4Chan and Quinn Respond to Gamergate Chat Logs,* ESCAPIST (Sept. 7, 2014), http://www.escapistmagazine.com/news/view/137293-Exclusive-Zoe-Quinn-Posts-Chat-Logs-Debunking-GamerGate-4Chan-and-Quinn-Respond [https://perma.cc/966L-KTPB]. These logs are not from 4Chan itself, but are logs from GamerGate chats regarding blackhat tactics from IRC, which also does not save logs. For 4chan and forum saved threads, see 4CHAN DATA, http://4chandata.org/ [https://perma.cc/26AB-PQV7]. This is an archive of 4chan threads without images. While there is a more recent 4chan thread archive with images, this author believes it is inappropriate to link to anything with active 4chan image macros.

307. *See* 4CHAN, *supra* note 8.

308. Other than the chatlogs referenced above, this author has not been able to find such explicit chatlogs. *See* discussion *supra* note 306.

309. *See* discussion *supra* Section II.C.

310. *See* discussion *supra* Section I.C.

311. *See supra* notes 4-5.

be.[312] In Justine Sacco's case,[313] the harassment she received in the period after her racist tweet became viral would be within the nexus, but harassing actions after she fell out of the Internet's attention span would not be.[314]

The most difficult problem is tying the actions of absent defendants to named defendants. After all, that is one of the difficulties the proposed civil conspiracy cause of action attempts to address. But the underlying basis of the agreement remains the same, that each of the actions taken by each of the participants was part of a larger attempt to hurt the victim. The extent of the agreement is a consideration. For example, cybermob participants who spread defamatory messages on the Internet may want to divorce themselves from the person who burns down the victim's home. Or with the *AutoAdmit* defendants, if the plaintiffs' Yale classmates who participated in the defamatory speech chose to vandalize their dorm room or attack them in the gym, should the others who merely posted that the plaintiff had a sexually transmitted disease be held liable? Probably not. These issues, involving the natural-and-probable consequences doctrine[315] and proximate causation,[316] need to be addressed, but are beyond the scope of this Note.

4. An Unlawful Act Committed to Further the Agreement

As part of their complaint, the plaintiffs listed a number of tortious actions by the *AutoAdmit* defendants. These include defamation and intentional infliction of emotional distress.[317] Any of these, if strong enough to survive a prima facie test, is sufficient to create the grounds for a civil conspiracy cause of action. Similarly, other cybermob targets are victims of defamation, intentional infliction of emotional distress, threats, and of real life harassment stemming from the same cybermob campaign. This Note's proposal considers its agreement element as being based on unlawful acts, so plaintiffs should also be able to establish this element.

---

312. *See* Lee, *supra* note 5.

313. *See* Ronson, *supra* note 15.

314. *Id.*

315. *See Natural and Probable Consequences*, 25 C.J.S. Damages § 34.

316. *See Cause*, BLACK'S LAW DICTIONARY (10th ed. 2014).

317. Complaint, Doe I v. Individuals, 561 F. Supp. 2d 249 (D. Conn. 2008) (No. 307CV00909 CFD).

5. Harm that Was Proximately Caused by Conspiracy

One of the plaintiffs alleged that she did not receive any offers from law firms because of the reputational harm caused by the defendants' defamatory speech.[318] Courts should find this proximate, because the alleged loss of employment opportunities resulted from Internet searches conducted by her employers; it would be foreseeable that posting defamatory material about someone could cause them to lose their job or render them unable to find a job.[319] Since the defamatory speech indicated in the complaint was the primary result of Internet searches for the plaintiff's name, the relationship should not be too attenuated for causation.[320] The other plaintiff alleged intentional infliction of emotional distress due, at least in part, to the various threats posted in the threads, especially those that indicated physical world proximity, such as claims of actually seeing her in the physical world or attending classes with her.[321] Assuming the threats were outrageous enough to qualify for intentional infliction of emotional distress, a court should find that the threats were a proximate cause of the distress.

This proposal limits liability to those who have committed tortious acts or who directly facilitated the campaign. Therefore, all of the harm that was the direct effect of those actions should meet the proximate causation element. That harm should be sufficient to meet the unmasking tests and allow plaintiffs their day in court. However, harm and the damages that result are one of the less defined elements of the proposed cause of action. This is purposeful in that it allows courts and juries to act as a check against overly expansive liability. This is necessary when the proposed cause of action allows victims to recover all of their damages through joint and several liability.

The biggest problem lies in determining the extent of damages, especially when a cybermob harassment campaign accompanies a mass shaming campaign. Dividing the extent of damage between the two may be impossible. But that is the realm of the jury, with the court acting to ensure that no award is outside of the bounds of justice.

---

318. *Id.*
319. *Id.*
320. *Id.*
321. *Id.*

B. Possible Inadequacies of Cybermob Civil Conspiracy

The fear with extending unmasking and liability theories to cybermob speech is the possibility of abuse, both as a matter of chilling speech and as tool for extortion. However, under the current unmasking regime, there is a certain amount of discretion allowed to courts. Courts may decide when they can or cannot assert personal jurisdiction. In both the *Dendrite* and *Mobilisia* tests, the balancing element allows for a great degree of discretion in regards to whether a given defendant can be unmasked, and whether the suit can proceed.[322] Furthermore, by forcing plaintiffs to set out the exact tortious wrongs upon which the cause of action is built, courts can limit abuse.[323] Courts can also choose to grant summary judgments based on proximate causation, holding that certain putative defendants' actions are too remote to incur liability. Courts can choose to sever defendants if the courts do not find agreement between parties.

A certain amount of activity chilling is desirable, because one of the purposes of this proposal is to deter unlawful, harmful speech.[324] One of the problems with civil conspiracy is the possibility that it is actually under-inclusive. Civil conspiracy requires a meeting of the minds, an active participation that does not address all cases of cybermob activity, such as the damage caused by negligent cybermob activity. Steven Rudderham[325] and the Australian Star Wars Dad[326] are examples of harm caused by cybermob activity that, in large part, does not seem malicious.[327] In both incidents, posts that falsely

---

322. *See supra* notes 145-49, 154, and accompanying text.

323. *See supra* notes 145-49, 154, and accompanying text.

324. *AutoAdmit*, ENCYCLOPEDIA DRAMATICA, https://encyclopediadramatica.se/AutoAdmit [https://perma.cc/V6CY-Q64Q] (last updated Mar. 27, 2017, 11:43 PM) ("Probably the only negative consequence of the LOLsuit [*AutoAdmit*] was the chilling effect it had on the board: many established posters, now twenty-something attorneys, were afraid to be discovered frequenting a forum characterized by the media as racist, misogynist, etc.").

325. *See* Webb, *supra* note 6.

326. *See* Michael & Crane, *supra* note 68.

327. *See* Webb, *supra* note 6; Michael & Crane, *supra* note 68. Both posts quickly became viral. This author assumes that the hundreds who shared the false allegations did so in good faith. At least in the Rudderham example, the reputational harm that drove him to suicide seemingly came from those close to him, who suddenly actually believed that Rudderham was a pedophile. In that case, the original poster should be held liable. Those who shared should not, and could not, be liable under American defamation law unless they were at least negligent, and in some jurisdictions, only if they were found to have been acting with either a reckless or knowing disregard for the post's truth, as the post would likely be considered one of public concern. Restatement (Second) of Torts § 580B (1977).

accused the victims of being pedophiles were shared by most in good faith. People were likely sharing to warn others; it is unlikely that those who shared the posts on social media would be held liable for defamation if they believe what they were sharing was the truth. While there may have been some malicious tortious action, the resulting reputational damage mostly arose from lawful sharing in good faith. The participants caused very real harm, and they acted similarly to a cybermob, in that they mobilized around a trigger event and cooperated in their actions that caused the harm.[328]

This Note also uses a nexus of time and trigger to show agreement, to bring the participants together so that civil conspiracy becomes viable. This cause of action does nothing for the victim who is the target of a single, persistent cyberstalker or cyberbully. Nor does it serve as an adequate remedy for those who may receive small amounts of cyber harassment over time, where the harm is in the aggregate and not the result of a large, impactful campaign.

This Note discussed other inadequacies and possible problems with the proposed cause of action.[329] Where possible, this Note addressed those limits and signaled when it does not have the answers. This Note further acknowledges that actual usage of its proposed cause of action is heavily dependent on local jurisdictions, because of the differences in long-arm statutes and civil conspiracy common law among different state jurisdictions. Nonetheless, this Note hopes to contribute to the discussion of cybermobs and possible solutions to the problem that cybermob harassment causes.

CONCLUSION

Internet harassment is and will continue to be a problem that an increasingly digitized world must address.[330] This Note's proposed civil conspiracy cause of action is one attempt at addressing part of that larger problem. In seeking to recompense victims and discourage antisocial behavior, this Note joins the larger discussion about the creation of norms on the Internet, about what constitutes acceptable behavior, and at what point the First Amendment gives way to an individual's right not to be harmed. Commentators often compare the Internet to the Wild West.[331] Just as civility and the rule of law eventually came to the Wild West, they can also be brought to

328. *See* Michael & Crane, *supra* note 68.
329. *See, e.g., supra* Section III.B.
330. *See generally* CITRON, *supra* note 19; Fisher, *supra* note 11.
331. *See*, *e.g.,* CITRON, *supra* note 19, at 17.

Internet, for the betterment of society as a whole and as a detriment to the outlaw—in this case, to the detriment of the troll.

The current situation is not tenable. The legal system has not yet adapted to the problems that the Internet brings to litigation.[332] Cyber harassment, especially cybermob harassment, is generally an unfamiliar problem for civil courts.[333] The Internet is relatively easy to access, widening the potential pool of perpetrators with little regard for the bounds of jurisdiction or geography.[334] The way that the Internet both connects users together into networks and creates persistence for cyberspace activities compounds cyber harassment harm.[335] Anonymity encourages wrongdoers and makes them harder to find.[336] The CDA shields the most obvious litigation targets, the intermediary ICSs that control the flow of content.[337] If cybermob victims want to recover their losses, victims must directly target their harassers.[338] To do so, victims must first unmask potential defendants, but some are impossible to identify or to exert jurisdiction over, while others do not have the resources to be viable defendants.[339] The lack of defendants leaves victims without a way to recover for their losses.[340] This is a gap in the law created by the novel nature of our increasingly digital reality.

The proposed civil conspiracy cause of action addresses some of these issues, creates a more viable way for victims to recover, and discourages participation in cybermob behavior.[341] Civil conspiracy creates grounds for joinder, extends the reach of long-arm statutes so that courts may establish in personam jurisdiction over defendants, and makes each defendant jointly and severally liable for the actions of the conspiracy.[342] Following in the path of criminal, antitrust, and civil law in the physical world, the proposed cause of action forces cybermob participants to incur liability when they join together with other participants to illicitly harm another.[343] The nexus of time and

---

332. *See, e.g., supra* Sections I.A-B.
333. *See, e.g., supra* Sections I.A-B.
334. *See* discussion *supra* Section I.B.3.
335. *See supra* notes 56-60 and accompanying text.
336. *See supra* notes 62-68 and accompanying text.
337. *See* discussion *supra* Section I.B.1.
338. *See* discussion *supra* Section I.B.
339. *See* discussion *supra* Sections I.B.1, I.B.3.
340. *See* discussion *supra* Sections I.B.1, I.B.3.
341. *See* discussion *supra* Section II.C.
342. *See* discussion *supra* Section II.C.
343. *See* discussion *supra* Section II.C.

trigger ties the cybermob's participants together while simultaneously limiting the problem of over-inclusion.[344]

Changing circumstances and developing technology creates gaps in the law. The challenge is to balance protection and freedom, to regulate while not letting "hard cases[] make bad law."[345] The proposed civil conspiracy cause of action is an attempt at striking that balance in a world where the distinction between physical space and cyberspace grows ever smaller.

344. *See* discussion *supra* Section II.C.

345. N. Sec. Co. v. United States, 193 U.S. 197, 364 (1904) (Holmes, J., dissenting).