COMMENTS

"Do(x) You Really Want to Hurt Me?": Adapting IIED as a Solution to Doxing by Reshaping Intent

Victoria McIntyre*

I. INTRODUCTION

Picture this: a woman goes on a date with a man she meets on OkCupid.[1] The first date goes well, and they begin seeing each other more frequently. She is a video game developer, and he is a computer programmer. The relationship does not last very long, and after five months they break up. But the man is not ready to let it go. Instead of moving on, he compiles a complete dossier of her personal information, including her phone number, email address, and home address. He also includes information he learned during their time together, drawn from personal Facebook messages, texts, and emails. He posts this record

* © 2016 Victoria Elizabeth McIntyre. Managing Editor, Volume 19, *Tulane Journal of Technology and Intellectual Property*. J.D. candidate 2017, Tulane University Law School; B.A. 2013, English, Union College. The author would like to thank her friends and family for their support and suggestions in writing this Comment, as well as the members of the *Journal* for their hard work and dedication.

1. OkCupid is an online dating service. OKCUPID, http://www.okcupid.com (last visited Mar. 18, 2016).

publicly online, claiming he only wanted to warn others about his ex-girlfriend.

In reality, he is hoping to reach out to people already inclined to attacking women online. By the time he publishes the post, he believes the odds that she will be harassed are 80%. He posts on two video game websites, and it quickly finds its way onto 4chan, an online community with a history of harassing women.[2] The first two websites delete the post, so he posts it himself on a WordPress blog.[3]

Immediately after the post is published, the woman receives emails from strangers calling her a slut. Her biography on Wikipedia is altered to read "Died: soon." Strangers send her crude photoshopped images of herself. There are hundreds of tweets demanding she kill herself. Not only has her personal reputation been damaged, but she has also received numerous death and rape threats from an anonymous mob who now have her personal information (and that of some of her family) not limited to her home address, phone number, emails, and passwords, but also including nude photos of her. Her voicemail is hacked, and a new message is recorded, her father is threatened, and her future employer is threatened until the company rescinds her job offer. She is forced to flee her apartment and hide in friends' homes, sleeping on couches. It is impossible to know who is behind the threats because they are able to hide behind various accounts on the Internet—anonymous and faceless.

And it does not stop there. To make sure that the post stays fresh, the man joins 4chan discussion boards, and releases additional information online, including her supposed current location and baseless theories about her sex life—accusing her of sleeping with critics in exchange for favorable game reviews.

These attacks start a dangerous, overt movement of misogyny in the video game industry. The original post is used as evidence that women are ruining the industry's boy's club. Within a week, anonymous online harassers are relentlessly harassing and threatening to kill other women in the industry, and releasing their private information online.

These are real threats, and these are real victims.[4] As of now, the law is not fully equipped to address this problem, let alone stop this

---

2. *See* Caitlin Dewey, *Absolutely Everything You Need To Know To Understand 4chan, the Internet's Own Bogeyman*, WASH. POST: INTERSECT (Sept. 25, 2014) (explaining how 4chan is an unusual and controversial forum, and providing examples of harassment of women).

3. WordPress is a free blog-hosting service. WORDPRESS, http://www.wordpress.com (last visited March 18, 2016).

4. These facts are all based on the real-life plight of Zoe Quinn and other women in the video game industry. *See generally*, Zachary Jason, *Game of Fear*, BOS. MAG. (May 2015), http://www.bostonmagazine.com/news/article/2015/04/28/gamergate/; Helen Lewis, *Gamergate:*

conduct. This Comment highlights the dangers of doxing (a form of Internet harassment) and how its initial act can lead to escalating harassment. This Comment also exposes the difficulty of providing legal remedies to doxing victims under existing laws, and suggests legislative and judicial solutions that can prevent this behavior while preserving Internet freedoms and First Amendment rights.

First, this Comment explains what doxing is, where it can lead, and whom it affects. Next, this Comment addresses gaps in existing law and other obstacles which prevent victims of doxing from receiving relief for their suffering. Lastly, this Comment offers the common law tort of intentional infliction of emotional distress (IIED) as a potential source of relief for doxing and addresses the ways IIED needs to change in order to provide a legal remedy to doxing victims. This Comment concludes by asserting that the consequences of doxing are so severe in nature, immediate action and cooperation by law enforcement, prosecutors, lawmakers, and judges is necessary to ensure doxing victims receive the relief they deserve.

II. WHAT IS DOXING?

Doxing is a form of harassment that normally occurs when an individual obtains (through deep Internet searching or hacking, generally) private information about a person such as their phone number, home address, or social security number, and posts this information online without permission.[5] The goal of doxing is to scare or intimidate a victim by posting the victim's confidential information online so that he or she becomes fearful about where the information may be posted next.[6]

Crash Override Network, an online task force (staffed by former targets, including Zoe Quinn, the woman this Comment's introduction is based on) that fights against online abuse, defines doxing as "the act of publishing someone's personal information, of which there would be a reasonable expectation of privacy and dubious value to the conversation,

---

A Brief History of a Computer-Age War, GUARDIAN (Jan. 11, 2015, 6:21 AM), http://www.theguardian.com/technology/2015/jan/11/gamergate-a-brief-history-of-a-computer-age-war. In 2014, in an incident referred to as "Gamergate," several women were doxed by male gamers trying to intimidate them into keeping silent about sexism in the video game industry. *See* Jason, *supra*; *see also* Lewis, *supra*.

5. *See* Sameer Hinduja, *Doxing and Cyberbullying*, CYBERBULLYING RES. CTR. (Sept. 16, 2015), http://cyberbullying.org/doxing-and-cyberbullying/; *see also Preventing Doxing*, CRASH OVERRIDE NETWORK (Jan. 17, 2015), http://crashoverridenetwork.tumblr.com/post/108387569412/preventing-doxing (detailing common ways in which anonymous mobs can gather an individual's data). Doxing is sometimes referred to as doxxing. Hinduja, *supra*.

6. Hinduja, *supra* note 5; *see also Preventing Doxing*, *supra* note 5.

in an environment that implies or encourages intimidation or threat."[7] The information released does not need to be difficult to find in the first place to be considered private.[8] As Crash Override explains, "[d]oxing is less about the availability of the information, and more about the way it is used to intimidate or harass a target."[9]

The term dox was first used as shorthand for "documents" by early computer hackers.[10] Derived from the slang "dropping dox," it was "an old-school revenge tactic that emerged from hacker culture in [the] 1990s."[11] Doxing (to refer to generally scornful identity-revelation) was first used in the 2000s to refer to the conduct of hackers who would compile an individual's personal and private information and release it publicly without the individual's consent.[12] Doxbin, a Tor[13] site used to host files containing the personal information of individuals and certain groups of people, was launched in 2011.[14] During this same time period, Anonymous, a hacker collective, also "adopted doxing as a 'harassment tactic.'"[15] Since then, the meaning of doxing has become less clear, as some journalists have co-opted the phrase to refer to "deep investigative reporting," "blurr[ing] the distinction between nefarious digital intrusion and noble journalism."[16] While not universal, there has been a "strong cultural taboo against doxing" among online communities like Reddit,[17] a news networking website where members can view and share content on virtually any topic.[18]

---

7. *So You've Been Doxed: A Guide to Best Practices*, CRASH OVERRIDE NETWORK (Mar. 21, 2015), http://crashoverridenetwork.tumblr.com/post/114270394687/so-youve-been-doxed-a-guide-to-best-practices [hereinafter, *So You've Been Doxed*].

8. *Id.*

9. *Id.*

10. Megan Garber, *Doxing: An Etymology*, ATLANTIC (Mar. 6, 2014), http://www.theatlantic.com/technology/archive/2014/03/doxing-an-etymology/284283/.

11. Mat Honan, *What Is Doxing?*, WIRED (Mar. 6, 2014, 1:03 PM), http://www.wired.com/2014/03/doxing/.

12. C.S-W, *What Doxxing Is, and Why It Matters*, ECONOMIST (Mar. 10, 2014, 11:50 PM), http://www.economist.com/blogs/economist-explains/2014/03/economist-explains-9.

13. Tor is an Internet network that provides anonymity to its users by hiding their IP addresses. *See Tor Overview*, TOR, http://www.torproject.org/about/overview.html.en (last visited Oct. 3, 2016).

14. Garber, *supra* note 10. Doxbin has since been shut down. *See* Patrick Howell O'Neill, *Dark Net Hackers Steal Seized Site Back from the FBI*, DAILY DOT (Nov. 10, 2014, 1:58 PM), http://www.dailydot.com/layer8/doxbin-dark-net/.

15. Garber, *supra* note 10.

16. C.S-W, *supra* note 12.

17. Honan, *supra* note 11.

18. *See* About page for Reddit, REDDIT, https://about.reddit.com/ (last visited Oct. 5, 2016).

A. Swatting: A Dangerous Offshoot of Doxing

> *[S]watting is the most troubling manifestation of online harassment, because it's not online at all—it's actual weapons and confusion, showing up at your door.*[19]

Swatting, (sometimes referred to more literally as SWATing) is an example of just how dangerous the wanton release of private information online can be. Swatting is when an individual files a false report (often by placing a fake 911 call) of a critical incident to create an emergency that will elicit an overwhelming response from law enforcement.[20] Typically, a swatter will claim that there is an ongoing hostage situation or bomb threat to trick emergency response teams into responding with SWAT teams or bomb squads.[21] The swatter will often use technology to bypass caller ID to pretend to be placing a distress call from the home or phone of the victim.[22] The swatter may also make the call online, masking his IP address by using virtual private networks.[23]

While swatting may occur independently from doxing, a swatting attack can be preceded by a dox or another kind of Internet harassment publicizing a victim's private information.[24] In these cases, a swatter uses personal information obtained through a dox, such as a victim's home address or phone number, to place the distress call or target the victim at that address.[25]

B. The Victims

According to a 2014 Pew Research Report, online harassment is a problem that affects many types of Internet users.[26] 73% of adult Internet users have witnessed someone be harassed in some form online, and

---

19. Jason Fagone, *The Serial Swatter*, N.Y. TIMES MAG. (Nov. 24, 2015), http://www.nytimes.com/2015/11/29/magazine/the-serial-swatter.html?_r=2.

20. *See Don't Make the Call: The New Phenomenon of 'Swatting*,' FBI (Feb. 4, 2008), https://www.fbi.gov/news/stories/2008/february/swatting020408.

21. Richard Lewis, *On Twitch, SWAT Teams Are Becoming Dangerous Props for Trolls*, DAILY DOT (Aug. 22, 2014 at 9:10AM), http://www.dailydot.com/esports/swatting-twitch-trend-prank/.

22. *See id.*

23. *See* Fagone, *supra* note 19.

24. *See, e.g.*, Alex Hern, *Gamergate Hits New Low with Attempts To Send Swat Teams to Critics*, GUARDIAN (Jan. 13, 2015, 9:57 AM), http://www.theguardian.com/technology/2015/jan/13/gamergate-hits-new-low-with-attempts-to-send-swat-teams-to-critics (discussing an incident in which Seattle-area police officers were sent to the home of a web developer after an anonymous tip was phoned in by Internet trolls).

25. *See id.*

26. *See* Maeve Duggan, *Online Harassment: Summary of Findings*, PEW RES. CTR. (Oct. 22, 2014), http://www.pewinternet.org/2014/10/22/online-harassment/.

40% have personally experienced it.[27] A more serious form of harassment—the type that comes with physical threats, stalking, and sexual harassment—is more often targeted at women.[28]

Among online adults, Pew's findings indicate:

> Young women, those 18-24, experience certain severe types of harassment at disproportionately high levels: 26% of these young women have been stalked online, and 25% were the target of online sexual harassment. In addition, they do not escape the heightened rates of physical threats and sustained harassment common to their male peers and young people in general.[29]

"Women and young adults were more likely to experience harassment on social media," and "men . . . were more likely to report online gaming sites as their source of harassment."[30] These findings likely correspond to demographics on gaming sites and do not mean women are not disproportionately harassed on these types of sites, too.[31] While the survey found most online environments were viewed as equally welcoming to both men and women, the starkest results were for online gaming environments, where 44% of respondents believed the platform is more welcoming toward men.[32]

In addition, the report found that "those who live out more of their lives online—whether for work, pleasure, or both—are more likely to experience harassment."[33] The type of job a person holds is relevant to his or her experiences with online harassment, as digital technology workers were more likely to report experiencing online harassment.[34] On one hand, this is logical: the more time one spends online, the more opportunity one has to experience online harassment. On the other hand, digital technology workers are predominately male, not female.[35]

In fact, Gamergate, the online harassment campaign forcing some high profile women in the gaming industry to leave their homes out of fear, essentially began when women advocated for greater inclusion

---

27. *Id.*
28. *Id.*
29. *Id.*
30. *Id.*
31. *See id.*
32. *Id.*
33. *Id.*
34. *Id.* "Almost half of those internet users who work in the digital technology industry (48%) said they had experienced online harassment." *Id.*
35. As of 2016, women hold only 24% of all tech jobs worldwide. *The Industry Gender Gap: Women and Work in the Fourth Industrial Revolution*, WORLD ECON. F. 1, 2 (Jan. 2016), http://www3.weforum.org/docs/WEF_FOJ_Executive_Summary_GenderGap.pdf.

within the industry.[36] "Traditionalists" on the other side eschewed change.[37] "The divide is, in part, demographic: It's the difference between the historical, stereotypical gamer—young, nerdy white guy who likes guns and boobs—and the much broader, more diverse range of people who play now."[38] Gamergate is about "drowning out critics of traditional, patriarchal, dude-dominated gaming culture."[39]

That said, as *Slate* writer Amanda Hess explains in *Why Women Aren't Welcome on the Internet*, "a woman doesn't even need to occupy a professional writing perch at a prominent platform to become a target. . . . [j]ust appearing as a woman online, it seems, can be enough to inspire abuse."[40] Hess describes an experiment conducted by the University of Maryland in 2006 where researchers set up fake online accounts, placed them into online chat rooms, and observed accounts with feminine usernames received an average of 100 sexually explicit or threatening messages per day; masculine names received only 3.7.[41] She goes on to explain that this "gendered harassment" cannot be ignored and "has severe implications for women's status on the Internet":

> Threats of rape, death, and stalking can overpower our [women's] emotional bandwidth, take up our time, and cost us money through legal fees, online protection services, and missed wages. I've spent countless hours over the past four years logging the online activity of one particularly committed cyberstalker, just in case. And as the Internet becomes increasingly central to the human experience, the ability of women to live and work freely online will be shaped, and too often limited, by the technology companies that host these threats, the constellation of local and federal law enforcement officers who investigate them, and the popular commentators who dismiss them—all arenas that remain dominated by men, many of whom have little personal understanding of what women face online every day.[42]

While this gendered problem exceeds the scope of this paper, the fact that a significant portion of the population is disproportionately targeted by online harassers highlights the need to address doxing.[43]

---

36. *See* Caitlin Dewey, *The Only Guide To Gamergate You Will Ever Need To Read*, WASH. POST (Oct. 14, 2014), https://www.washingtonpost.com/news/the-intersect/wp/2014/10/14/the-only-guide-to-gamergate-you-will-ever-need-to-read/.

37. *Id.*

38. *Id.*

39. *Id.*

40. Amanda Hess, *Why Women Aren't Welcome on the Internet*, PAC. STANDARD MAG. (Jan. 6, 2014), http://www.psmag.com/health-and-behavior/women-arent-welcome-internet-72170.

41. *Id.*

42. *Id.*

43. *See* Duggan, *supra* note 26.

III. GAPS IN THE LAW

The methods used to gather information, and the acts carried out with such information, can dictate whether a court finds the act of doxing legal. If the information is obtained legally and posted publicly, without explicitly threatening someone, a court might consider the act legal, despite the poster knowing or expecting their posting of this information will cause severe emotional distress to the victim.[44] However, if it can be proven that the information was obtained illegally through hacking, the doxing may be punishable under criminal law.[45]

Once the information is available online, it is much easier for the original release of personal information to facilitate illegal activity. Consequently, while courts might not consider forms of doxing, such as posting an individual's phone number online, illegal,[46] a doxer could be charged with aiding and abetting identity theft if he or she publishes someone's social security number.[47] A doxer could also be criminally charged if the dox leads to harassment or stalking.[48]

---

44. *See, e.g.*, Chan v. Ellis, 770 S.E.2d 851, 852 (Ga. 2015) (holding that insufficient evidence existed to prove that the defendant contacted the plaintiff without her consent under the state stalking statute, even though defendant and fellow commentators "have published nearly 2,000 posts about [plaintiff], many of which are mean-spirited, some of which are distasteful and crude, and some of which publicize information that [plaintiff] would prefer not to be so public. . . . At least one post . . . threaten[s] to publicize additional information about [the plaintiff] and her family").

45. *See Computer Crime Statutes*, NAT'L CONF. ST. LEGISLATORS (May 12, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx (providing a list of computer crime and hacking statutes).

46. *See, e.g.*, Slibeck v. Union Oil Co. of Cali., 1986 WL 11542, at *1 (Del. Super. Ct. Sept. 18, 1986) (holding that because phone numbers are generally publicly available, a plaintiff has no privacy interest in its publication). In *Wilson v. Harvey*, the court of appeals in Ohio found that when a student's phone number and email address were available on his university directory, he "had no reasonable expectation of privacy involving this information because it was published in various forms obtainable by university students and faculty." Wilson v. Harvey, 842 N.E.2d 83, 91 (Ohio Ct. App. 2005). The defendants had created a flyer "depicting [the plaintiff] as a homosexual" looking for a companion. *Id.* at 86. The defendants listed the plaintiff's name, email address, phone number, and a picture of him on the flyer.

However, in *Benz v. Washington Newspaper Publishing Co.*, the court found that "[a]lthough plaintiff's phone numbers and addresses may be available to the public on the internet and in phone books, that does not negate the fact that the information are nonetheless private facts." Benz v. Wash. Newspaper Pub. Co., No. 05-1760 EGS, 2006 WL 2844896, at *8 (D.D.C. Sept. 29, 2006). The court distinguished between posting phone numbers "in a website listing CNN producers or in a media bulletin or in any such site" with posting the information "for solicitation purposes" on a site for individuals seeking sex, as was done in *Benz*. *Id.* The court found the latter conduct resulted in a claim for public disclosure of private facts. *Id.*

47. *See* United States v. Sutcliffe, 505 F.3d 944 (9th Cir. 2007).

48. *See* Marlisse Silver Sweeney, *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/ ("[I]n states with specific cyber

A. Criminal Law Penalties

There are advantages to addressing doxing through criminal law. Prosecutors hired by the government, and not private actors hired by victims, bring charges against criminals,[49] ensuring that victims are not barred from bringing a suit due to high legal costs. A criminal conviction can also provide emotional relief to a victim if he or she sees a harasser sent to jail.[50] Bringing a successful criminal action against a harasser has the potential to create a deterrent effect, making future would-be harassers wary to engage in the same actions for fear of similar consequences.[51]

That said, many criminal remedies are not appropriate for an act of doxing that has not yet progressed beyond the specific targeting of a victim and the release of his or her personal information online.[52]

For example, stalking, while a potential criminal charge for some engaged in doxing,[53] does not encompass all initial instances of doxing. Stalking is normally defined under state law as "threats made with intent to place another person in imminent fear of grave bodily injury in connection with a malicious 'course of conduct' that would cause a reasonable person to suffer substantial emotional distress."[54] While a doxing victim may reasonably fear for his or her life, and doxing most certainly can be malicious conduct that results in emotional distress, it can be difficult for the state to prove the required elements of stalking.[55] Doxing may not present explicit threats of bodily injury.[56] Threats of injury and emotional distress made online, assuredly very distressing,

---

stalking and harassment laws like California, Illinois, and Massachusetts, theoretically victims can press criminal charges against their online stalkers and harassers.").

49. *See* 4 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 13.1(a) (4th ed. 2015).

50. The government's job in a criminal trial is to protect the interests of the state, not the interests of the victim, and the two interests may not always align. DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 123 (2014).

51. *See id.*

52. While I believe that this act, if targeted and with the specific intent to cause an individual severe distress, could, and in some cases, should be considered a crime in its own right, I attempt to make the distinction that simply releasing someone's personal information online is not currently a crime. While the information that the actor releases could lead to greater harassment and other crimes, I address only the original dox here.

53. *See* CITRON, *supra* note 50, at 124 ("Federal stalking and harassment laws capture a wide range of online abuse.").

54. *Id.* at 124.

55. *See id.*

56. As explained earlier, Crash Override Network defines doxing as simply "the act of publishing someone's personal information, of which there would be a reasonable expectation of privacy and dubious value to the conversation, in an environment that implies or encourages intimidation or threat." *So You've Been Doxed*, *supra* note 7.

may not be tangible enough for a prosecutor to prove guilt beyond a reasonable doubt.[57]

Harassment, on the other hand, is generally understood to be "a willful and malicious 'course of conduct' directed at a person that would cause a reasonable person to suffer substantial emotional distress and that does cause the person to suffer distress."[58] However, state harassment statutes can vary widely in the conduct that they prohibit:

> Over the past twenty years, every state has to some extent updated its laws related to stalking and harassment to keep pace with technological change. Some statutes reach abuse perpetrated via particular technologies such as e-mail. Other statutes cover only abuse directly communicated to victims. Only a few states prohibit harassment communicated directly or indirectly, on- or offline.[59]

In addition, some state harassment and stalking laws may only apply to abuse that is communicated *directly to the victim*.[60]

For example, in 2013, Ian Barber was charged with aggravated harassment and "dissemination of an unlawful surveillance image in the second degree"[61] for allegedly posting his then-girlfriend's nude photos on Twitter and emailing them to her boss and sister.[62] The aggravated harassment claim was dismissed because New York state law required that Barber send the harassment (in this case, the nude photos) directly to the victim.[63]

The dissemination claim was also dismissed because the law, the court found, "requires more than the mere posting of an image on a social networking site such as Twitter or the sending of an image [to] other persons."[64] In so finding, the court relied on a 2008 New York case in which the defendant used a camera phone to record himself (without the plaintiff's knowledge, permission, or authority) having sexual intercourse with the plaintiff and to send that video to at least one other

---

57. *See* CITRON, *supra* note 50, at 123 ("Threats must be unequivocal, unconditional, and specific. Victims typically need to feel tangible, sustained, and immediate fear.").

58. *Id.* at 124.

59. *Id.*

60. *See* N.Y. PENAL LAW §§ 240.40(1)(a), 250.55 (McKinney 2014).

61. *Id.* § 250.55.

62. *See* People v. Barber, No. 2013NY059761, WL 641316, at *1 (N.Y. Sup. Ct. Feb. 18, 2014).

63. *Id.* at *5 ("Clearly, it is essential to a charge of Penal Law § 240.40(1)(a) that the defendant undertake some communication with the complainant.").

64. *Id.* at *3.

person.[65] The defendant in the 2008 New York case was likewise not found culpable under the same law.[66]

Sending the nude photos to his former girlfriend's boss and sister, even though it seems obvious that a reasonable person could conclude that this conduct would adversely affect her relationships and cause her severe distress, proved to be innocent behavior in terms of New York criminal law.[67] Moreover, even if Barker's conduct had fallen under a harassment statute, the consequences may have been relatively slight; while stalking may sometimes be a felony, harassment is usually a misdemeanor and imposes only limited sentences and fines.[68]

Further, doxing as it is defined in this Comment most certainly does not fit within a statute prohibiting abuse communicated directly to victims.[69] "[C]yber harassers generate grave fear and emotional distress without sending communications to victims—something legislators could not have fully appreciated when they adopted harassment and stalking laws."[70] Finally, prosecutors may also be reluctant to engage in the work and devote the resources required to find an anonymous perpetrator if the act is only a misdemeanor and they do not believe this is the best use of resources.

Federal stalking and harassment statutes may sometimes be available to victims. However, the interstate stalking statute can have the same application problems to doxing as a state statute.[71] The Federal Telecommunications Act protects against threats and harassment that occur interstate (especially applicable when conduct is occurring on the Internet), but it also has its limitations.[72] The only provision that could seemingly apply to doxing is § 223(a)(1)(C), which prohibits an individual from "utiliz[ing] a telecommunications device . . . without

---

65. *Id.* (citing People v. Morriale, 20 Misc. 3d 558 (Crim. Ct. NY County 2008)).

66. *Morriale*, 20 Misc. 3d at 561.

67. While I could continue to discuss various state law statutes incapable of providing relief to victims of cyber abuse, that goes beyond the scope of this Comment. I instead simply offer this anecdote to illustrate the problems that exist in terms of criminalizing this conduct.

68. *See generally* SUSAN PRICE, OFFICE OF LEGISLATIVE RESEARCH, OLR BACKGROUNDER: CYBERSTALKING, 1-6 (2012).

69. As noted earlier, doxing occurs when an individual's personal information is posted online to a large audience or another individual, but not specifically to the victim. Hinduja, *supra* note 5.

70. CITRON, *supra* note 50, at 143.

71. *See* 18 U.S.C. § 2261A(2) (2012). This statute also requires a "course of conduct" that is defined as "a pattern of conduct composed of 2 or more acts, evidencing a continuity of purpose." *See* 18 U.S.C. § 2266 (2012). This could also pose problems with finding liability if the doxing does not happen in a pattern, or if an attacker simply doxes all of a victim's information all at once and there is no need to engage in a pattern.

72. *See* 47 U.S.C. § 223 (2012).

disclosing his identity and with intent to abuse, threaten, or harass any specific person."[73] This statute could also pose problems: does using an Internet handle or username qualify as disclosing one's identity? What if law enforcement is unable to *ever* disclose his true identity?

California has passed a solicitation law prohibiting the distribution or publication of personal identifying information with intent to place a victim in reasonable fear for his or her safety.[74] This law seems to have had some success: in *People v. Shivers*, the defendant was convicted under section 653.2 for electronically distributing a harassing message via Twitter.[75] The message indicated that the defendant had a restraining order against the victim and that the victim was stalking him and making death threats against him.[76] Part of the code provision requires that a person intend to "imminently caus[e] that other person unwanted physical contact, injury, or harassment, by a third party."[77] In *Shivers*, this was satisfied because it could be inferred that the defendant "knew that persons who encountered [the victim] after reading his tweets could have been motivated to report her to the police for what they believed was her stalking him, or to otherwise harass her."[78] It is unclear whether an individual who publicly distributed personal information only with intent to harass, and without the fear of being reported to the police, would likewise be convicted.[79] Further, the code provision requires a clear intent, which could be difficult to prove.[80]

California's legislation is a step in the right direction, and other states ought to revise their state laws to account for the online environment in which today's cyber abuse takes place. While statutory revision is necessary, it can take a long time to pass legislation and affect change. As such, this Comment does not solely advocate for that approach.

---

73. 47 U.S.C. § 223(a)(1)(C) (2012).

74. CAL. PENAL CODE § 653.2 (West 2012).

75. *See* People v. Shivers, 186 Cal. Rptr.3d 352, 354 (Cal. Ct. App. 2015).

76. *Id.* at 355.

77. PENAL § 653.2.

78. *See Shivers*, 186 Cal. Rptr. 3d at 357.

79. This statute is still relatively new (effective as of January 1, 2010), and I have been unable to find any cases in which this occurs.

80. Snehal Desai, *Smile for the Camera: The Revenge Pornography Dilemma, California's Approach, and Its Constitutionality*, 42 HASTINGS CONST. L.Q. 443, 467-68 (2015) (noting that "[t]hough the reasoning behind the posting . . . might be to cause the victim emotional distress, a perpetrator might be able to escape liability if he proves that his primary aim was not to cause emotional distress"). This is another reason why I advocate for the use of IIED, which accounts for recklessness or negligence. *See* discussion in *infra* Part IV.

B. Issues with Law Enforcement and Prosecutors

Criminal penalties, in addition to presenting potential proof and application issues, depend upon law enforcement and prosecutors to take the victim's complaints seriously in order to succeed.[81] Law enforcement can be behind the curve in terms of their knowledge and ability to trace down offenders:

> At times, officers resist dealing with victims' reports for the same reasons that laypeople refuse to take online harassment seriously. The majority of law enforcement agencies do not investigate cyber stalking complaints because they lack training to understand the seriousness of the attacks, the technologies used to perpetrate them, and the usefulness of existing laws.[82]

In *Hate Crimes in Cyberspace*, Danielle Citron provides multiple examples of law enforcement's inadequate response to victims of cyber abuse, including multiple reports of police officers telling a victim "to ignore the abuse because the posters were 'just boys being boys,'" that "annoying and immature Internet communications did not meet the criteria for criminal prosecution,"[83] or that "it's not a big deal. It's just online talk," when referring to a poster's threatening comments on a blog.[84] She also describes officers who were unable to determine perpetrators' identities: "the officers 'barely understood e-mail, let alone the cybersleuthing needed to unravel international IP addresses and anonymous comments.'"[85]

When *Slate* writer Amanda Hess approached law enforcement after being threatened on Twitter, an officer asked her, "What is Twitter?"[86] When *Time* journalist Catherine Mayer reported a bomb threat lodged against her, the officers she encountered "thought usernames were secret

---

81. *See* LaFave, *supra* note 49, at § 13.2(a), (b) (explaining police and prosecutorial discretion to seek a prosecution). While civil suits will likely involve law enforcement, law enforcement generally plays a much smaller role in civil litigation because the action is brought privately. *See* 1 WENDELL H. GAUTHIER & DANIEL G. ABEL, LITIGATING TORT CASES § 1:7 (2015) (discussing the private attorney's role in instigating a civil tort action); 5 EVA MARIE MANCUSO & SONJA L. DEYOE, LITIGATING TORT CASES § 57:9 (2015) (discussing the use of private investigators as opposed to local law enforcement with respect to a civil tort action).

82. CITRON, *supra* note 50, at 84.

83. *Id.* at 87.

84. *Id.* at 88.

85. *Id.* While it may in some cases be impossible to identify a perpetrator's identity, I include this quote to highlight the even greater difficulties in doing so when unfamiliar with the Internet, in general. Further, as Hess notes: "If police don't know whether the harasser lives next door or out in Nebraska, it's easier for them to categorize the threat as non-immediate. When they treat a threat as a boyish hoax, the implication is that the threat ceases to be a criminal offense." Hess, *supra* note 40.

86. Hess, *supra* note 40.

codes and didn't seem to know what an IP address was," ultimately advising her to simply get offline.[87] In addition, as Hess points out in *Why Women Aren't Welcome on the Internet*, the majority of law enforcement is male, and thus less likely to have experienced online harassment.[88] Without My Consent, an organization working to combat online invasions of privacy has sections on their website entitled, "The police say this is not a crime, and won't pursue the matter" and "How do I present my case to law enforcement?" highlighting the prevalence of the problem and providing alternatives to incorrect or ignorant responses that law enforcement may provide to a victim of online abuse.[89]

Apart from the potential to being charged with a crime, social norms may deter a doxer from posting information online. A doxer may experience social harm as a result of his or her act of doxing, especially on an online community like Reddit.[90] However, doxing's prevalence today suggests that the social harms that may befall the doxer, such as public reprimands and disappointment from other online community members, are not enough to thwart this conduct.[91] This, combined with the fact that many of the legal remedies currently available are ineffective because they require the plaintiff to show specific harm or apply only to the after effects of doxing (should they escalate) and not to the initial act

---

87. *Id.*

88. *Id.*

> The Internet is a global network, but when you pick up the phone to report an online threat, whether you are in London or Palm Springs, you end up face-to-face with a cop who patrols a comparatively puny jurisdiction. And your cop will probably be a man: According to the U.S. Bureau of Justice Statistics, in 2008, only 6.5 percent of state police officers and 19 percent of FBI agents were women. The numbers get smaller in smaller agencies. And in many locales, police work is still a largely analog affair: 911 calls are immediately routed to the local police force; the closest officer is dispatched to respond; he takes notes with pen and paper.

Id.

89. *Conversations To Have with Your Lawyer*, WITHOUT MY CONSENT, http://withoutmyconsent.org/resources/conversations-have-your-lawyer# (last visited Mar. 17, 2016).

90. *See* Andrew Beaujon, *Redditors Furious Newsweek 'Doxxed' Bitcoin Founder*, POYNTER (Mar. 6, 2014), http://www.poynter.org/2014/redditors-furious-newsweek-outed-bitcoin-founder/242348/ ("[O]n Reddit, 'doxxing' [releasing personal information about someone] is a cardinal sin.").

91. That said, the social harms of being accused of doxing have been enough to motivate some to bring defamation suits. *See* Brennan v. Stevenson, No. JKB-15-2931, 2015 WL 7454109, at *1 (D. Md. Nov. 24, 2015) (reviewing a case in which the plaintiff brought a defamation claim after the defendant authored an article in which she accused the plaintiff of "harassing and doxing trans women on [the Plaintiff's] websites").

of doxing,[92] illustrates the need to use and broaden IIED claims to address doxing.

C. Tort Law Remedies

Tort law may also provide victims of doxing with a remedy by allowing victims to receive damage awards from their harassers. The tort of public disclosure of private facts, for example, is an option.[93] Under this tort, an individual is liable if he publicizes private information that "would be highly offensive to a reasonable person" and "is not of legitimate concern to the public."[94] However, public disclosure of private fact, by definition, is not an option if the facts are not considered "private."[95] Further, it cannot apply when the public has a legitimate interest in the potentially embarrassing, but truthful, private facts, as is likely the case if the facts concern a celebrity or public figure.[96]

The tort of IIED allows a plaintiff to impose liability for any extreme and outrageous conduct that causes severe emotional harm.[97] While the standard of "extreme and outrageous" may be more difficult to meet than other previous discussed torts, IIED has the ability to address the targeted publication of personal information without the limitations of other torts.[98]

There are of course downsides to bringing a civil tort action. Civil suits can be expensive and victims are forced to bear the costs of bringing the suit:

> Having lost their jobs due to online abuse, they cannot pay their rent, let alone the fees for attorneys and computer-forensic specialists. Even if victims can afford to sue their attackers, they may be reluctant to do so if

---

92. For example, a stalking or harassment statute would only encompass the conduct that occurs through use of the personal information, not the actual release of the information. *See* CITRON, *supra* note 50, at 123-24.

> Under state law, stalking is usually defined as threats made with intent to place another person in imminent fear of grave bodily injury in connection with a malicious "course of conduct" that would cause a reasonable person to suffer emotional distress. Harassment is typically understood as a willful and malicious "course of conduct" directed at a person that would cause a reasonable person to suffer substantial emotional distress and that does cause the person to suffer distress.

Id.

93. *See* RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1977).

94. *Id.*

95. *See id.*

96. *See id.*

97. RESTATEMENT (THIRD) OF TORTS: PHYSICAL & EMOTIONAL HARM § 46 (AM. LAW INST. 2012).

98. *See id.*

> their attackers have few assets. It may not be worth spending time and resources suing someone who is effectively judgment-proof.[99]

Another concern is that a victim may be required to bring suit in his or her real name, rather than under a pseudonym.[100] If a victim has to file under his or her real name and his or her complaint is made available online, the victim may be subject to further embarrassment or abuse.[101] This puts victims in a very difficult situation.[102]

IV. A LEGAL SOLUTION: EXPANSION OF INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS

The most difficult issue in devising a way to punish and prevent doxing is to find a way to provide victims with legal relief while preserving freedom of speech. This Part suggests that the tort of IIED provides a way for victims to bring suits against their attackers. It will also address the limitations of this tort claim and what lawmakers and courts should do to modernize laws to deal with doxing and other forms of online harassment. This Part ultimately argues that IIED has the most room to expand to provide relief to victims of doxing.

A. A History of IIED

The Third Restatement of Torts defines IIED as: "[a]n actor who by extreme and outrageous conduct intentionally or recklessly causes severe emotional harm to another is subject to liability for that emotional harm and, if the emotional harm causes bodily harm, also for the bodily harm."[103] In the Restatement comments, the authors explain that courts have found liability for IIED only where the defendant's conduct has been extreme *and* outrageous.[104] The specific facts and circumstances of the case at hand must show that the conduct did more than intentionally or recklessly cause emotional harm.[105] This "double limitation" of extreme *and* outrageous "requires both that the character of the conduct be outrageous and that the conduct be sufficiently unusual to be

---

99. CITRON, *supra* note 50, at 122.

100. *Id.*

101. *See id.*

102. *See id.* "They can seek justice but risk exacerbating their suffering or let injustices stand with some privacy intact. Some victims would rather give up their claims than give the harassment more publicity." *Id.*

103. RESTATEMENT (THIRD) OF TORTS: PHYSICAL & EMOTIONAL HARM § 46 (AM. LAW INST. 2012).

104. *Id.* cmt. d.

105. *Id.* "Specific rules for when conduct is extreme and outrageous cannot be stated, nor can categories of conduct be identified for formulation into universal rules." *Id.*

extreme."[106] The Restatement comments further note that "even if emotional harm is inflicted for no purpose other than to cause such harm, some degree of emotional harm must be expected in social interaction and tolerated without legal recourse."[107] Therefore, an actor is only liable under the "extreme and outrageous" requirement if the conduct extends "beyond the bounds of human decency such that it would be regarded as intolerable in a civilized community."[108] Ordinary insults, annoyances, indignities, and threats are not enough to impose liability (even if the actor seeks to inflict emotional harm) in order to provide space for an individual's freedom to express negative opinions or other exercises of freedom of speech.[109]

To prove intent, a plaintiff must prove that the defendant intended to inflict severe emotional harm to the plaintiff or that the defendant acted with reckless disregard as to whether the plaintiff would suffer severe emotional harm:

> An actor intends severe emotional harm when the actor acts with the purpose of causing severe emotional harm or acts knowingly that severe emotional harm is substantially certain to result. An actor acts recklessly when the actor knows of the risk of severe emotional harm (or knows facts that make the risk obvious) and fails to take a precaution that would eliminate or reduce the risk even though the slight relative to the magnitude of the risk, thereby demonstrating the actor's indifference.[110]

Intent can be evidenced through words, conduct, or the specific circumstances by which events occurred.[111] An actor who, instead of harming the intended victim, harms a third party, may still satisfy the element of intent through the doctrine of transferred intent.[112] However, courts have generally limited liability for IIED to bystanders who were present at the time of the conduct and who were also close family members of the victim.[113]

---

106. *Id.*
107. *Id.*
108. *Id.*
109. *Id.*
110. *Id.* cmt. h.
111. Catherine Palo, *Proof of Intentional Infliction of Emotional Distress*, *in* 136 AM. JURIS. PROOF OF FACTS 3D § 15 (2016).
112. Restatement (Third) of Torts: Physical & Emotional Harm § 46 cmt. i (Am. Law Inst. 2012).
113. *Id.*

B. The First Amendment

The Supreme Court has addressed IIED in terms of the right to exercise freedom of speech, noting that the Free Speech Clause of the First Amendment[114] may be used as a defense to state tort claims of IIED.[115]

In *Snyder v. Phelps*, the Supreme Court placed the right to protest in a public space and exercise freedom of speech above the IIED claim of a grieving father.[116] When the Westboro Baptist Church protested at the funeral of a fallen United States soldier with placards reading "Thank God for Dead Soldiers," "You're Going to Hell," "God Hates Fags," and "God Hates You," the Court deemed Westboro's actions legal.[117] It found that the issues the signs highlighted, i.e. "the political and moral conduct of the United States and its citizens, the fate of our Nation, homosexuality in the military" were matters of public import.[118]

Although Westboro's speech was conducted at a funeral setting, this did not change the fact that it was speech "at a public place on a matter of public concern [and] that speech is entitled to 'special protection' under the First Amendment."[119] The Court made clear that "[s]uch speech cannot be restricted simply because it is upsetting or arouses contempt."[120] It ignored the jury's finding that Westboro's picketing was "outrageous" and that Westboro was liable for IIED, holding that "[w]hat Westboro said, in the whole context of how and where it chose to say it, is entitled to 'special protection' under the First Amendment, and that protection cannot be overcome by a jury finding that the picketing was outrageous."[121]

The Court specifically chose to note that Westboro's picketing did not involve any "pre-existing relationship or conflict between Westboro and [the father] that might suggest Westboro's speech on public matters was intended to mask an attack on [the father] over a private matter."[122] Additionally, in a footnote the Court noted that, "an Internet posting may raise distinct issues in [an IIED] context."[123] This footnote suggests that

---

114. U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech.").
115. Snyder v. Phelps, 562 U.S. 443, 443-44 (2011).
116. *Id.* at 459.
117. *Id.* at 448, 460.
118. *Id.* at 454.
119. *Id.* at 458.
120. *Id.*
121. *Id.*
122. *Id.* at 455.
123. *Id.* at 499 n.1.

"the published word aimed at a particular individual may not be protected in the same way [as it was in *Snyder*]."[124] This reading makes *Snyder* a narrow opinion "that did not necessarily address claims based upon more directed, emotionally harmful speech."[125] If this interpretation is correct, this means that doxers and actors who engage in targeted speech could be held liable for IIED in spite of *Snyder*'s overwhelming protection of freedom of speech.[126]

The district court for the Northern District of Alabama distinguished the Supreme Court's interpretation of IIED in *Snyder* in *Holloway v. America Media, Inc.*[127] In *Holloway*, the mother of Natalee Holloway, a teenager who disappeared during a senior trip to Aruba and was never found, sued the *National Enquirer* for IIED.[128] She alleged that the *National Enquirer* published multiple articles "that were knowingly false and which were intended by defendants to cause [the plaintiff] to suffer severe emotional distress."[129] The court noted that the case required it to "draw a line between the state's right to protect a citizen from outrageous conduct and invasions of privacy, and the Constitutional protection of free speech guaranteed by the First Amendment."[130] In doing so, the court looked to the Supreme Court's holding in *Snyder*, reading it as finding that First Amendment protection "does not extend to speech . . . that is used as a weapon simply to mount a personal attack on someone over a private matter."[131]

In its holding, the court focused on the "knowingly false speech" made by the *National Enquirer* (which may not be at issue in a doxing situation where private but true information is publicized), but it also placed great weight on "actual malice," noting that this type of conduct, "motivated by a specific intent to cause emotional harm to a particular

---

124. AMY GAJDA, THE FIRST AMENDMENT BUBBLE: HOW PRIVACY AND PAPARAZZI THREATEN A FREE PRESS 69 (2015).

125. *Id.*

126. *See id.*

127. *See* Holloway v. American Media, Inc., 947 F. Supp. 2d 1252, 1261-62 (N.D. Ala. May 22, 2013) (distinguishing *Snyder*, 562 U.S. at 458).

128. *Holloway*, 947 F. Supp. 2d at 1254.

129. *Id.*

> The articles described a map that purported to show where Natalee's body was located, a "secret graveyard" where Natalee had been "buried alive," and other details about her "murder" and the treatment of her "corpse," including that it had been secreted temporarily in a coffin with another corpse before being moved to a final location.

Id.

130. *Id.* at 1259.

131. *Id.* at 1262; *see also* Snyder v. Phelps, 562 U.S. 443, 455 (2011).

person may also fall outside First Amendment protection."[132] This concept of "actual malice" provides a framework for other courts to distinguish *Snyder* from cases such as those involving doxing victims in which the speech is not false. Unfortunately, *Holloway* was settled out of court so it was never heard by an appellate court and remains only persuasive, not binding precedent.[133] Still the court's analysis and reading of *Snyder* provides a framework for other courts to follow.

The status of the entity or individual responsible should not determine the legality of doxing, which causes severe emotional harm. Does it make a difference that it was the "National Enquirer" that published the information in *Holloway* and not a specific individual? Mathew Ingram raises this issue in another context: *Newsweek* doxing the alleged creator of Bitcoin, Satoshi Nakamoto.[134] Ingram compares what news agencies like *Newsweek* do to the things individuals are doing on Reddit and other forums, asking, "are these things really so different?"[135] He explains:

> *Newsweek* included many personal details about Nakamoto, including his work history and details about his extended family, and even his personal health—and they posted a photo of his home, one in which you could clearly see his address and the licence [sic] plate on his car. What if that man isn't even the "real" Satoshi Nakamoto? Then an elderly man in poor physical health has been mis-identified [sic] as a Bitcoin multimillionaire, something that could have very real repercussions for him and his family.[136]

Does the legitimate public interest in the founder of Bitcoin extend to the details about Nakamoto's extended family, personal health, and physical location?[137] The journalist who doxed Nakamoto has since said on

---

132. *Holloway*, 947 F. Supp. 2d at 1263.

133. *See* Kent Faulk, *Natalee Holloway's Mother Settles Lawsuit with National Enquirer*, ALABAMA.COM (Aug. 6, 2013, 4:04 PM), http://blog.al.com/spotnews/2013/08/natalee_holloways_mother_settl.html.

134. Mathew Ingram, *Of Bitcoin and Doxing: Is Revealing Satoshi Nakamoto's Identity Okay Because It Was Newsweek and Not Reddit?*, GIGAOM (Mar. 6, 2014, 10:43 AM), https://gigaom.com/2014/03/06/of-bitcoin-and-doxxing-is-revealing-sakamotos-identity-okay-because-it-was-newsweek-and-not-reddit/.

135. *Id.*

136. *Id.* (referencing Leah McGrath Goodman, *The Face Behind Bitcoin*, NEWSWEEK, (Mar. 6, 2014, 6:05 AM), http://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html.)

137. Forbes journalist Kashmir Hill also weighs in:

> Is it fair to say that it's an invasion of privacy to prove that a man who identified himself as Satoshi Nakamoto when he created Bitcoin is in fact a man named Satoshi Nakamoto? He created something that has become a global phenomenon, caused governments to wring their hands, and taken on immense real-world value, with a billions-dollar market cap. The need to know the creator, who himself holds much of

Twitter that she needed to include the details she did to "offer a sense of his humanity," arguing that what she did was not an invasion of privacy because the photo of his residence and car were already public.[138] While she may have simply released publicly available personal information, she made this information easily accessible to many people, an act that is not without privacy and potential safety concerns for Nakamoto. Whether or not the doxing occurs at the hands of a journalist or scornful individual, if the information made available has the ability to cause severe emotional distress, it should be encompassed under an IIED claim.

C. How IIED Must Change

IIED is not a new tort, but courts are still working out its boundaries.[139] The Restatement explains that IIED began as a "catchall" to provide a cause of action for conduct that did not fit within any other torts and that might otherwise go unremedied.[140] IIED ought to now act again as a "catchall," providing relief to victims of doxing who cannot find relief elsewhere. Original concerns with IIED were that the tort would allow plaintiffs to extend liability to false claims or trivialities.[141] Though the tort of IIED has been recognized by courts, victims still face difficulties in proving liability.

Of all the elements of IIED, intent seems to be most difficult to prove in terms of doxing. How do you prove that an individual who simply posts personal information does so with the intent to, or with reckless disregard towards inflicting severe emotional distress on the victim? To confront this issue, this Comment proposes a reworking of the intent analysis, based on the Supreme Court precedent set forth in *Snyder*, and the Alabama district court's decision in *Holloway*, to

---

> the currency, was important. This is not tabloid journalism; this is very much in the public interest, and important for those adopting and investing in the Bitcoin system to know.

Kashmir Hill, *The Outing of Bitcoin Creator Satoshi Nakamoto Is Important Journalism*, FORBES (Mar. 6, 2014, 11:57 AM), http://www.forbes.com/sites/kashmirhill/2014/03/06/the-outing-of-bitcoin-creator-satoshi-nakamoto-is-brilliant-journalism/#4a3026dbb359.

138. Leah McGrath Goodman (@truth_eater), TWITTER (Mar. 6, 2014, 6:50 AM) http://twitter.com/truth-eater/status/44158G733256560640; *see also* Leah McGrath Goodman (@truth_eater), TWITTER (Mar. 6 2014, 7:02 AM) http://twitter.com/truth-eater/status/441589607076216832 (tweeting "@EntropyExtropy Good question. Pictures and info people are asking about (including residence and car) already public. His name too.#Bitcoin").

139. RESTATEMENT (THIRD) OF TORTS: PHYSICAL & EMOTIONAL HARM § 46 (AM. LAW INST. 2012).

140. *See id.* cmt. a.

141. William L. Prosser, *Intentional Infliction of Mental Suffering—A New Tort*, 5 CURRENT LEGAL THOUGHT 391, 397 (1939).

encompass the external factors at play with a targeted act like doxing that occurs entirely online.

In order to protect freedom of speech, and to prevent the punishing of individuals who post personal, but more limited information for legitimate purposes,[142] this Comment suggests that courts take a balancing approach by using of a totality of the circumstances test. This Comment proposes that when hearing a doxing claim of IIED, courts consider and balance the totality of five factors equally: the prior relationship between parties, whether the personal information is accompanied by other inflammatory information or calls to action, where the information is posted, the amount of personal information included, and whether the information is a matter of public importance.

First, courts should consider the prior relationship between parties when determining intent. In *Snyder*, the Supreme Court specifically noted the lack of relationship or conflict as evidence that Westboro's speech was not a masked attack over a private matter.[143] In *Holloway*, the court also noted that specific intent to cause harm to a particular person falls outside the First Amendment and can be grounds for IIED.[144] Based on these interpretations, an existing prior relationship between parties, though not determinative, should be highly relevant and support a finding of intent.

Second, courts should consider whether the personal information is accompanied by any other inflammatory information or calls to action when determining intent. For example, if an individual posts a victim's home address and phone number online, referring to the victim as a "slut" or a "bitch," this should support a finding of intent and indicate that this is more directed, emotionally harmful conduct. Additionally, if an individual posts the same information accompanied by instructions to others to spam the victim, threaten her, harass her, etc., this should support a finding of intent.

Third, where the information is posted should be a consideration when determining intent. If the information is posted on a site like 4chan or Doxbin, or a forum specifically aimed at harassing people, this should support a finding of intent.

Fourth, courts should consider the amount of information included in the post when determining intent. If an individual posts nothing more

---

142. Legitimate purposes may be limited to civic engagement, reaching out to elected officials, and sending get-well cards to sick children.

143. Snyder v. Phelps, 562 U.S. 443, 455 (2011).

144. Holloway v. American Media, Inc., 947 F. Supp. 2d 1252, 1263 (N.D. Ala. May 22, 2013).

than a phone number and an email address, this would not contribute to a finding of intent. If he were to post this information as well as her home address, license plate, parents' home address, parents' phone numbers, etc., this conduct, while likely legal on its own, would support a finding of intent.

Finally, the fifth factor should preserve the matter of public importance issue addressed in *Snyder* when determining intent.[145] This factor serves as a safeguard to freedom of speech, but because it is only one of five factors, it is not determinative and cannot unfairly tip the scales in one way or another. Since determining whether a matter is of public importance is inherently subjective, it is better served when balanced equally amongst other more objective factors. If the information posted is a matter of public importance, this should not contribute to a finding of intent.

With a better understanding of the current atmosphere in which doxing is occurring, lawmakers and courts have the ability to place doxing within the definition of IIED, making a statement that the consequences of doxing are more than on par with IIED's threshold of extreme and outrageous conduct. In addition, by adopting this Comment's proposed five-factor totality of the circumstances test to determine intent, courts have the ability to hone in on the language provided in *Snyder* and *Holloway* to find that the targeted publication of personal information against an individual (doxing) qualifies as IIED. While doxing may not be the kind of conduct that the Supreme Court was anticipating in *Snyder*, or Alabama in *Holloway*,[146] in certain cases it can be, and it should be illegal.

V. CONCLUSION

Doxing is a prevalent problem that does not yet occupy an explicit space within criminal statutes or tort law. Many law enforcement officers, judges, and prosecutors believe that the response to doxing is simple: get off the Internet.[147] This is an unreasonable solution in 2016 where so much of our daily lives involve being online and connected in some way. In order to deter and address the problem of doxing, courts need to recognize the severe emotional distress that can accompany doxing and work to broaden IIED to allow it to serve as a remedy. To do that, courts should follow the five-factor totality of the circumstances test

145. *See Snyder*, 562 U.S. at 455.
146. *See id.*; *see also Holloway*, 947 F. Supp. 2d at 1263.
147. Hess, *supra* note 40.

proposed by this Comment when analyzing intent in a doxing suit. Courts ought to balance the following factors: (1) the prior relationship between the parties; (2) the speech accompanying the information posted; (3) the location of the post; (4) the amount of information posted; and (5) whether the information is a matter of public importance. Distinctions will still need to be drawn amongst these factors in terms of which circumstances support a finding of intent, but this approach provides a way for doxing victims to overcome difficulties in proving intent. It offers a compromise between addressing the severe consequences of doxing to victims and maintaining the right to exercise freedom of speech.