Fordham Law Review

Volume 85 | Issue 5 Article 21

2017

The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information

Julia M. MacAllister
Fordham University School of Law

Follow this and additional works at: https://ir.lawnet.fordham.edu/flr

 Part of the Courts Commons, Criminal Law Commons, Internet Law Commons, and the Legislation Commons

Recommended Citation

Julia M. MacAllister, *The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information*, 85 Fordham L. Rev. 2451 (2017).
Available at: https://ir.lawnet.fordham.edu/flr/vol85/iss5/21

This Note is brought to you for free and open access by FLASH: The Fordham Law Archive of Scholarship and History. It has been accepted for inclusion in Fordham Law Review by an authorized editor of FLASH: The Fordham Law Archive of Scholarship and History. For more information, please contact tmelnick@law.fordham.edu.

THE DOXING DILEMMA: SEEKING A REMEDY FOR THE MALICIOUS PUBLICATION OF PERSONAL INFORMATION

*Julia M. MacAllister**

In recent years, malevolent actors have seized upon a new tool to harass, silence, threaten, and injure people online: doxing—the malicious publication of personal identifying information like a home address. Although doxing is an online tool, it causes concrete and serious harm to victims by moving harassment from the Internet to the physical world. Congress and state legislatures have begun to address different forms of cyberharassment. However, no effective and consistent legal remedy for doxing currently exists. This Note examines and critiques current federal and state schemes, and it ultimately proposes that lower federal courts should adopt a new intent standard to make the federal Interstate Communications Statute more applicable to doxing and that states can and should criminalize malicious doxing.

* J.D. Candidate, 2018, Fordham University School of Law; A.B., 2008, Dartmouth College. Thank you to Professor Joel Reidenberg for his guidance, and thank you to my family and friends, especially to my mom and dad, for their love and support—it takes a village.

INTRODUCTION

On the night of October 10, 2014, a Twitter user named "Death to Brianna" began to tweet rape and death threats targeted at Brianna Wu, head of development at independent game studio Giant Spacekat.[1] The user's picture, appearing next to each tweet, was a photo of Wu and her husband.[2] The user described in graphic detail how he planned to rape, murder, and mutilate Wu, kill her children, and torture her husband imminently.[3] Within four minutes of the harassment starting, the user

1. Caitlin Dewey, *In the Battle of Internet Mobs vs. the Law, the Internet Mobs Have Won*, WASH. POST (Feb. 17, 2016), https://www.washingtonpost.com/news/the-intersect/wp/2016/02/17/in-the-battle-of-internet-mobs-vs-the-law-the-internet-mobs-have-won [https://perma.cc/J7N9-8LF5].

2. Brianna Wu (@Spacekatgal), TWITTER (Oct. 10, 2014, 8:57 PM), https://twitter.com/Spacekatgal/status/520739878993420290/ [perma.cc/VK5M-SLPP].

3. *Id.*

wrote: "Guess what bitch? I now know where you live. You and Frank live at [home address redacted]."[4]

Fearing for her life, Wu fled her home in the middle of the night with her family.[5] Her harassers have not been charged.[6] Wu, like many other people who use the Internet daily,[7] had been doxed.[8] Doxing is a form of cyberharassment[9] involving the public release of personal information that can be used to identify or locate an individual, such as a home address, email address, phone number, social security number, and employer or school contact information.[10]

The injuries suffered by victims of cyberharassment are well documented: "post-traumatic stress disorder, depression, and serious emotional distress[,] . . . 'changes in sleeping and eating patterns, nightmares, hyper-vigilance, anxiety, helplessness, fear for safety, and shock and disbelief.'"[11] Thus, the law creates penalties for some types of cyberharassment such as threats transmitted over state lines,[12] stalking,[13] and swatting[14] (a wrong-premises SWAT raid of an innocent person's home[15]). However, this Note argues that the current statutory and common

---

4. *Id.*

5. *Id.*

6. Anna Merlan, *The Cops Don't Care About Violent Online Threats. What Do We Do Now?*, JEZEBEL (Jan. 29, 2015, 3:10 PM), http://jezebel.com/the-cops-dont-care-about-violent-online-threats-what-d-1682577343 [https://perma.cc/VU56-R7TE].

7. *See* Abby Ohlheiser, *The Leslie Jones Hack Used All the Scariest Tactics of Internet Warfare at Once*, WASH. POST (Aug. 26, 2016), https://www.washingtonpost.com/news/the-intersect/wp/2016/08/26/the-leslie-jones-hack-used-all-the-scariest-tactics-of-internet-warfare-at-once (describing the doxing and racist harassment that Leslie Jones faced after appearing in the film *Ghostbusters*) [https://perma.cc/24WR-2WMX]; Adi Robertson, *Trolls Drive Anita Sarkeesian out of Her House to Prove Misogyny Doesn't Exist*, VERGE (Aug. 27, 2014, 3:41 PM), http://www.theverge.com/2014/8/27/6075179/anita-sarkeesian-says-she-was-driven-out-of-house-by-threats (reporting that a feminist critic and her parents were doxed after she posted videos "aggregating and analyzing games that portray women as damsels in distress, ornamental eye candy, incidental victims, and other archetypes that tend to be written in service of and subordinate to male players and characters") [perma.cc/YD76-4DLY].

8. Dewey, *supra* note 1.

9. Cyberharassment enables actors "to harass their victims on a scale never before possible," with their conduct having both an "immediate effect" and "global dissemination." John B. Major, *Cyberstalking, Twitter, and the Captive Audience: A First Amendment Analysis of 18 U.S.C. § 2261A(2)*, 86 S. CAL. L. REV. 117, 126 (2012).

10. *See* Mary Anne Franks, Professor, Univ. of Miami Sch. of Law, Remarks at the American Bar Association Program on Doxing, Swatting, Trolls, and SJWs: Harassment and Gender Discrimination on Social Media Platforms (Nov. 8, 2016) (on file with the *Fordham Law Review*).

11. Major, *supra* note 9, at 126 (quoting Nicolle Parsons-Pollard & Laura J. Moriarty, *Cyberstalking—What's the Big Deal?*, *in* CONTROVERSIES IN VICTIMOLOGY 103, 108 (Laura J. Moriarty ed., 2d ed. 2008)).

12. *See* 18 U.S.C. § 875(c) (2012).

13. *See id.* § 2261A.

14. *See* CAL. PENAL CODE § 148.3 (West 2014) (criminalizing the act of making fraudulent emergency calls to cause SWAT raids of an innocent person's home).

15. *See* Rex M. Shannon III, Comment, *Nightmare on Your Street: Moving Towards Justice for Innocent Victims of Wrong-Premises SWAT Raids*, 77 MISS. L.J. 669, 670–72 (2007).

law regime fails to provide a reliable remedy for doxing victims.[16] Specifically, the law does not address situations in which an actor uses doxing for purely malicious purposes, such as revenge, harassment, or stalking, as opposed to political purposes or internal regulation.

Of course, some or all of the dispersed information might already be public information.[17] However, the semipublic nature of this information should not provide blanket immunity for a malicious actor who wields an individual's personal information as a tool to harass, threaten, intimidate, and injure that person.

In addition, the complex and intangible nature of doxing should not act as an excuse for lack of regulation, because "[t]oday, with smartphones and endless social media platforms, there is no difference between online and offline life. It is all just life."[18] In fact, when an actor doxes an individual—as opposed to harassing that individual in person—the harms caused by that harassment are amplified due to the conduct's "permanent quality that real world conduct lacks."[19] Moreover, doxing can incite individuals other than the actor to commit or threaten real-world violence because it entails the distribution of a subject's personal information to a broad and unknowable audience.[20] Indeed, experts warn that "[a]s people realize what an effective attack [doxing] can be, and how an individual can use the tactic to do considerable damage, . . . we're going to see a lot more of it."[21] Accordingly, a remedy for doxing is needed.

This Note examines the vast injuries doxing causes when used for purely malicious reasons and assesses whether an appropriate and successful legal remedy for this form of doxing can exist. Part I defines doxing, narrows the scope of this Note to "punching down" doxing, and examines the underlying doctrines of privacy and First Amendment law. Next, Part II analyzes the strengths and weaknesses of three relevant federal laws—the

16. *See* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 19 (2014) ("Victims are told not to expect any help: 'This is the INTERNET folks. . . . There are no laws here, at least not clearly defined ones.'" (alteration in original)). *But see, e.g.*, H.B. 225, 61st Leg., Gen. Sess. (Utah 2016) (cybercrime statute amendments).

17. *See* Franks, *supra* note 10.

18. *See* Marissa Lang, *Revenge Porn Is Target of Intimate Privacy Protection Act*, S.F. CHRON. (Sept. 30, 2016, 8:22 PM), http://www.sfchronicle.com/business/article/Intimate-Privacy-Protection-Act-to-take-on-9517671.php (quoting the author of revenge porn legislation Representative Jackie Speier) [https://perma.cc/JCG5-D7YK].

19. Major, *supra* note 9, at 126.

20. *See, e.g.*, Jason Slotkin, *"Pizzagate" Suspect Planned "Possibly" Violent Raid, Investigators Say*, NPR (Dec. 13, 2016, 3:22 PM), http://www.npr.org/sections/thetwo-way/2016/12/13/505424283/pizzagate-suspect-faces-federal-charge (describing a man who, motivated by a baseless Internet rumor, went to a Washington, D.C., restaurant and fired an assault rifle) [https://perma.cc/TZS2-24HN]. *See generally* Matthew James Enzweiler, *Swatting Political Discourse: A Domestic Terrorism Threat*, 90 NOTRE DAME L. REV. 2001, 2007 (2015) (discussing prank 911 calls resulting in heavily armed SWAT team responses to subjects' homes, and noting that "the risk of injury or death is beyond question in these instances").

21. Bruce Schneier, *The Rise of Political Doxing*, SCHNEIER ON SECURITY (Nov. 2, 2015, 6:47 AM), https://www.schneier.com/blog/archives/2015/11/the_rise_of_pol.html [https://perma.cc/4Y6G-R6U5].

Communications Decency Act, the Interstate Communications Statute, and the Interstate Stalking Statute—and a proposed bill. Part II also assesses the strengths and weaknesses of state criminal and common law approaches to cyberharassment and discusses the efficacy of these approaches to doxing. Then, Part III offers a blended solution and proposes that (1) federal courts should adopt the recklessness standard left open by the U.S. Supreme Court in *Elonis v. United States*[22] and (2) states can and should create or amend criminal laws addressing doxing because the doxing of a subject's home address is a true threat and thus can be regulated under the true threat exception to the First Amendment.

I. DROPPING DOX: UNDERSTANDING THE PROBLEM AND ITS UNDERLYING DOCTRINES

Part I.A defines doxing and distinguishes it from other types of cyberharassment, and Part I.B discusses the three ways actors could use doxing as a tool for harassment. Specifically, Part I.B narrows the focus of this Note to instances in which actors use doxing for purely malicious reasons, as opposed to political purposes or internal regulation. Finally, Part I.C introduces two rights that are directly affected by doxing: the right to privacy and the First Amendment's right to freedom of speech.

A. Doxing Defined

While the term's origin is not certain, "doxing" likely dates back to 2001 and the hacker group known as Anonymous.[23] "'Dox' is a longstanding shortening of 'documents' or 'to document,' especially in technology industries."[24] Scholars and journalists define "doxing" in various ways because it is not a defined legal term.[25] In an effort to apply a more

22. 135 S. Ct. 2001 (2015).

23. Bruce Schneier, *Doxing as an Attack*, SCHNEIER ON SECURITY (Jan. 2, 2015, 7:21 AM), https://www.schneier.com/blog/archives/2015/01/doxing_as_an_at.html [https://perma.cc/VL4R-5VC2].

24. Grant Barrett, Opinion, *Words of 2012*, N.Y. TIMES (Dec. 22, 2012), https://nyti.ms/2kBAuDs [https://perma.cc/4ED5-VVGV].

25. For example, Sarah Jeong defines doxing as "the publication of a physical residential address, or information protected by law." Sarah Jeong, *Stop Diluting the Definition of "Dox,"* SARAHJEONG DOT NET (July 8, 2015), https://sarahjeong.net/2015/07/08/stop-diluting-the-definition-of-dox/ [https://perma.cc/6Y3P-AS4W]. Gabriella Coleman, however, does not limit her definition of doxing to legally protected information; rather, she defines doxing as "the leaking of private information—such as Social Security numbers, home addresses, or personal photos." GABRIELLA COLEMAN, HACKER, HOAXER, WHISTLEBLOWER, SPY 7 (2015). Similarly, Danielle Keats Citron notes that doxing can occur when "[t]rolls post individuals' phone numbers, addresses, and social security numbers." CITRON, *supra* note 16, at 53. "Trolls" refers to persons who post deliberately erroneous or antagonistic messages to a newsgroup or similar forum with the intention of eliciting a hostile or corrective response. COLEMAN, *supra*, at 32 (defining trolls as "agents of cultural digestion [who] scavenge the landscape, re-purpose the most offensive material, then shove the resulting monstrosities into the faces of an unsuspecting populace"). Further, Bruce Schneier defines doxing as "the practice of publishing personal information about people without their consent." Schneier, *supra* note 23.

inclusive definition of doxing, this Note adopts Professor Mary Anne Frank's definition:

> The public release of an individual's private, sensitive, personal information, such as:
> - Home address, email address, phone number
> - Social security number
> - Employer and employer contact info
> - Family member's contact info
> - Photos of victim's children and the school they attend.[26]

This definition of doxing concerns publicly available information that would not necessarily require a hack to access.[27] In addition, this Note adopts the term "actor" to describe the person who doxes and the term "subject" to describe the person who is doxed.

Doxing rarely occurs in isolation.[28] Rather, doxing is often used as a tool by multiple actors within a greater campaign to harass one subject.[29] Actors dox in conjunction with other forms of harassment, such as revenge porn[30] and swatting.[31] However, these other forms of cyberharassment are distinguishable from doxing because they involve conduct rooted in older areas of law such as copyright[32] and manipulation of technology integrated in telecommunications channels.[33] Statutes concerning cyberharassment often draw directly from original offline stalking and harassment laws.[34]

---

26. Franks, *supra* note 10.

27. The Computer Fraud and Abuse Act (CFAA) criminalizes the misuse of a computer or the use of a computer in excess of a user's authorization. 18 U.S.C. § 1030 (2012). This statute could be used to prosecute actors who dox private information acquired by hacking. *See, e.g.*, Sarah A. Constant, *The Computer Fraud and Abuse Act: A Prosecutor's Dream and a Hacker's Worst Nightmare—The Case Against Aaron Swartz and the Need to Reform the CFAA*, 16 TUL. J. TECH. & INTELL. PROP. 231, 241 (2013) (discussing the case against a defendant who hacked JSTOR, an academic articles subscription service, and made articles available for free online). Doxing cases that do not involve a hack are not prosecutable under this statute.

28. *See* COLEMAN, *supra* note 25, at 44.

29. *See id.* Coleman describes Anonymous's 2010 harassment of Jessi Slaughter, a preteen video blogger. This harassment included "publish[ing] her phone number, address, and Twitter username, inundating her with hateful emails and threatening prank calls, circulating photoshopped images of her and satiric remixes of her videos." *Id.* She ultimately became an online "object of ridicule," forever associated with the term "lulzcow . . . whore." *Id.*; *see also Jessi Slaughter*, URBAN DICTIONARY (July 15, 2010), http://www.urbandictionary.com/define.php?term=Jessi+Slaughter&defid=5099483 [https://perma.cc/3JAZ-56HU].

30. *See* Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1098–99 (9th Cir. 2009) (describing the doxing of Cecilia Barnes in conjunction with the publication of pornographic photos taken without her consent).

31. *See* Kevin Poulsen, *Blind Hacker Sentenced to 11 Years in Prison*, WIRED (June 29, 2009, 7:28 PM), https://www.wired.com/2009/06/blind_hacker/ (discussing Matthew Weigman's confession to making "hundreds of false calls to police that sent armed SWAT teams bursting into the homes of [his] enemies") [https://perma.cc/QRC7-28GV].

32. Layla Goldnick, *Coddling the Internet: How the CDA Exacerbates the Proliferation of Revenge Porn and Prevents a Meaningful Remedy for Its Victims*, 21 CARDOZO J.L. & GENDER 583, 610 (2015).

33. Enzweiler, *supra* note 20, at 2004.

34. Nancy Leong & Joanne Morando, *Communication in Cyberspace*, 94 N.C. L. REV. 105, 114–15 (2015).

Many harassment laws were drafted in the 1990s when the Internet's usage was dramatically different from today.[35] In 1997, 18 percent of Americans used the Internet; today, 87 percent do.[36] Accordingly, the scale of harm doxing causes today is much greater than when legislatures drafted many applicable statutes.

In addition, doxing concerns the release of information that could otherwise be publicly available, unlike revenge porn and swatting.[37] By doxing a subject's home address or other information that can be used to locate a subject, an actor moves the harassment from the Internet into the physical world, putting the subject in actual physical danger. In addition, doxing makes personal information more accessible to the entire Internet, increasing the harassment by putting the subject at risk of injury or violence from a large audience in a way that other forms of harassment do not.[38] Nonetheless, in many cases, other forms of harassment are redressable, but there is no consistent legal remedy for doxing.[39]

B. Doxing Actors and Their Intent; Doxing Subjects and Their Injuries

Doxing is a tool, and the intent behind its use determines the proper approach for analyzing it. For the purpose of seeking a remedy, this Note recognizes three categories of doxing determined by the actor's intent: (1) punching down doxing (i.e., doxing for purely malicious purposes); (2) doxing for political purposes; and (3) the use of doxing by members of anonymous online communities as a tool for internal regulation (i.e., "unmasking"). Understanding the different actors who use doxing, the subjects who suffer the consequences of the publication of their personal information, and the varying motivations underpinning the use of doxing helps to narrow the search for an effective remedy.

1. Punching Down: Doxing "for the Lulz," or Worse

When an actor publishes a subject's personal information for purely malicious reasons, such as revenge, harassment, stalking, or "for the lulz" (meaning "laughter at the expense or the misfortune of others"[40]), the actor is engaging in punching down doxing. The public, viral, and instant nature

35. *See id.*

36. Monica Anderson & Andrew Perrin, *13% of Americans Don't Use the Internet. Who Are They?*, PEW RES. CTR. (Sept. 7, 2016), http://www.pewresearch.org/fact-tank/2016/09/07/some-americans-dont-use-the-internet-who-are-they/ [https://perma.cc/WP5B-LLWW].

37. *See supra* note 25 and accompanying text.

38. Schneier, *supra* note 21.

39. *See, e.g.*, Enzweiler, *supra* note 20, at 2001; Patricia R. Recupero, *New Technologies, New Problems, New Laws*, 44 J. AM. ACAD. PSYCHIATRY & L. 322, 325 (2016).

40. COLEMAN, *supra* note 25, at 31. "The lulz show how easily and casually trolls can upend our sense of security by invading private spaces and exposing confidential information. . . . [A]ny information thought to be personal, secure, or sacred is a prime target for sharing or defilement . . . ." *Id.* at 32–33.

of the Internet makes doxing an effective tool for harassing individuals for purely malicious purposes; it allows the actor to injure the subject on a much larger scale than in-person harassment. However, most people do not see doxing as a serious problem, because names and phone numbers are available in public phone directories.[41] Even so, huge differences in scale and accessibility exist between information "buried in small font in a dense book of which only a few thousand copies exist in a relatively small geographic location" and information released online that anyone anywhere in the world can access.[42]

For example, Cecilia Barnes's ex-boyfriend engaged in punching down doxing, among other forms of cyberharassment, against Barnes after she ended their long-term relationship.[43] He created a Yahoo! profile using her name that included sexual solicitations and nude photographs taken without her knowledge or permission.[44] In terms of doxing, Barnes's ex-boyfriend posted her personal and work telephone numbers, her home address, and her email address.[45] He solicited sex in Yahoo! chat rooms, impersonating her "and then directing the attention of male chat room goers to the indecent profiles he had posted of her."[46] Because her ex-boyfriend had doxed her by posting her personal information, Barnes began receiving harassing emails and phone calls, and random men attempted "to make personal visits to her [home] with the false expectation that Barnes would act upon the online sexual advances propagated by her ex-boyfriend."[47]

Barnes sued Yahoo! for negligently failing to remove the unauthorized profile after she tried to have the company take down the offensive material.[48] However, because the Communications Decency Act shields Internet service providers from liability, the case was dismissed.[49]

Revenge porn and other sexual material is offensive, humiliating, and can cause reputational damage. Further, the actual dox of Barnes's name and contact information is harassment that put her in physical danger and provoked fear for her safety. Barnes's ex-boyfriend had posted her personal contact information for the "specific purpose of committing a 'dangerous, cruel, and highly indecent' attempt at revenge," and such conduct ultimately resulted in significant harm to Barnes.[50] And yet, Barnes lacked any remedy for such conduct because the law fails to criminalize punching down doxing.

---

41. Katherine Cross, *"Things Have Happened in the Past Week": On Doxing, Swatting, and 8Chan*, FEMINISTING (Jan. 16, 2015), http://feministing.com/2015/01/16/things-have-happened-in-the-past-week-on-doxing-swatting-and-8chan/ [https://perma.cc/VWP5-TC7L].

42. *Id.*

43. *See* Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1098 (9th Cir. 2009).

44. *Id.*

45. Kimberly Quon, *Implementing a Standard of Care to Provide Protection from a Lawless Internet*, 31 WHITTIER L. REV. 589, 592 (2010).

46. *Id.*

47. *Id.*

48. *Barnes*, 570 F.3d at 1099.

49. *Id.* at 1105–06.

50. Quon, *supra* note 45, at 589.

Another example of punching down doxing is the "#gamergate" campaign of harassment ("Gamergate") that targeted women with threats of death and rape, general abuse, and the release of names, cell phone numbers, addresses, usernames, and parental information.[51] The actors worked together under the adopted moniker "Gamergate" and executed a "weekslong campaign to discredit or intimidate outspoken critics of the male-dominated gaming industry and its culture."[52] The subjects of Gamergate harassment, like Brianna Wu,[53] endured a constant barrage of harassment that affected their ability to work, socialize, and sleep.[54] Writer and developer Zoe Quinn fled her home after people online made rape and death threats toward her and bragged about putting dead animals through her mailbox.[55] Feminist cultural critic Anita Sarkeesian canceled a talk at Utah State University after the university administration received an email that a shooting massacre would be carried out at the event.[56] One important factor unites the stories of Barnes, Wu, Quinn, and Sarkeesian: the actors doxed them with the intent to intimidate, harass, silence, and threaten them. These stories exemplify punching down doxing, and this Note seeks legal relief for these subjects.[57]

---

51. A_Man_in_Black, *A #gamergate Harassment Sampler*, STORIFY, https://storify.com/a_man_in_black/gamergate-harassment (last visited Mar. 25, 2017) [https://perma.cc/Y5J8-LKF7].

52. Nick Wingfield, *Feminist Critics of Video Games Facing Threats in "Gamergate" Campaign*, N.Y. TIMES (Oct. 15, 2014), http://nyti.ms/1quzTvM [https://perma.cc/93GA-CWSA].

53. *See supra* notes 1–10 and accompanying text. The tweets targeting Wu read: (1) "Guess what bitch? I now know where you live. You and Frank live at [home address redacted]"; (2) "I've got a K-Bar [knife used by U.S. Marines] and I'm coming to your house so I can shove it up your ugly feminist cunt"; (3) "I'm going to rape your filthy ass until you bleed, then choke you to death with your husband's tiny Asian penis"; (4) "How's that for terrifying you stuck up cunt? I'm sick of you fucking feminist asshats"; (5) "Your mutilated corpse will be on the front page of Jezebel tomorrow and there isn't jack shit you can do about it"; (6) "If you have any kids, they're going to die too. I don't give a fuck. They'll grow up to be feminists anyway"; (7) "I hope you enjoy your last moments alive on this earth. You did nothing worthwhile with your life"; and (8) "You just made a shitty game nobody liked. That's it. Nobody [will care] when you die." Wu, *supra* note 2.

54. A_Man_in_Black, *supra* note 51.

55. Keith Stuart, *Zoe Quinn: "All Gamergate Has Done Is Ruin People's Lives,"* GUARDIAN (Dec. 3, 2014, 9:00 AM), https://www.theguardian.com/technology/2014/dec/03/zoe-quinn-gamergate-interview [https://perma.cc/GF65-RXL6].

56. Wingfield, *supra* note 52.

57. Cyberharassment disproportionately affects women and minority populations. *See* CITRON, *supra* note 16, at 13 ("Of the 3,393 individuals reporting cyber harassment to [advocacy group Working to Halt Online Abuse] from 2000 to 2011, 72.5 percent were female."); *see also id.* at 11 (arguing that young people, people of color, and lesbian, gay, bisexual, transgender, and queer (LGBTQ) people are more likely to experience severe emotional distress from cyberharassment). Statistics from suicide prevention organizations indicate that suicide rates by victims of online harassment are higher for minority populations. *Id.* (information on suicide statistics); *id.* at 80 (domestic violence history); *id.* at 102 (stalking).

2. Doxing for Political Purposes

This Note focuses on instances in which doxing is used for purely malicious purposes, as discussed in Part I.B.1; however, doxing is also used for political purposes. That is, some actors use doxing as a tool to increase transparency, expose what they perceive as injustice, or bring to light newsworthy information in the public interest. The subjects of this category of doxing might include multinational corporations, the U.S. military, Donald Trump, or racist police officers.

For example, in early 2010, Chelsea Manning doxed the U.S. military by releasing hundreds of thousands of sensitive military and diplomatic documents to WikiLeaks.[58] Manning dropped the dox because she "felt that the Iraq and Afghanistan 'war diaries' . . . were vital to the public's understanding of the two interconnected counter-insurgency conflicts."[59] The dox "provide[d] 'visual evidence of the gross abuse of state and military power.'"[60] Thus, Manning doxed for political purposes—rather than for purely malicious reasons.

Another well-known instance of doxing for political purposes occurred when the *New York Times* published an excerpt from then-presidential candidate Donald Trump's 1995 tax returns to show that "he had taken a huge [financial] loss in 1995 that could have allowed him to avoid paying federal income taxes for nearly two decades."[61] The *New York Times* dropped the dox for political purposes, stating that it was in the public interest because Trump "ha[d] broken with decades-long tradition and refused to make his returns public" during a presidential campaign.[62]

In addition, chapters of the Black Lives Matter network used doxing to expose police officers who purportedly used police brutality or racist tactics.[63] In these cases, the actors doxed to help protect other activists and

---

58. Chelsea E. Manning, *The Years Since I Was Jailed for Releasing the "War Diaries" Have Been a Rollercoaster*, GUARDIAN (May 27, 2015, 10:43 AM), https://www.theguardian.com/commentisfree/2015/may/27/anniversary-chelsea-manning-arrest-war-diaries [https://perma.cc/79ZZ-3JY4].

59. *Id.* Manning was convicted of the leak in 2010, and President Barack Obama commuted her sentence in January 2017. Charlie Savage, *Chelsea Manning to Be Released Early as Obama Commutes Sentence*, N.Y. TIMES (Jan. 17, 2017), https://nyti.ms/2k1jene [https://perma.cc/A6LC-4ZVT].

60. COLEMAN, *supra* note 25, at 83 (quoting Christian Christensen, *Collateral Murder and the After-Life of Activist Imagery*, MEDIUM (Apr. 14, 2014), https://medium.com/@ChrChristensen/collateral-murder-and-the-after-life-of-activist-imagery-3fc2accd82bb#.70lzgt8mt [https://perma.cc/M6ZJ-ZLTU].

61. Susanne Craig, *The Time I Found Donald Trump's Tax Records in My Mailbox*, N.Y. TIMES: TIMES INSIDER (Oct. 2, 2016), http://www.nytimes.com/2016/10/03/insider/the-time-i-found-donald-trumps-tax-records-in-my-mailbox.html [https://perma.cc/2RGQ-2PSE].

62. *Id.*

63. *See* J. Patrick Coolican, *Minneapolis City Council Member Alondra Cano Under Fire for Posting Phone Numbers, E-mail Addresses of Constituents*, STAR TRIB. (Dec. 24, 2015, 12:34 PM), http://www.startribune.com/minneapolis-city-council-member-alondra-cano-under-fire-for-posting-phone-numbers-email-addresses-of-constituents/363470421/ [https://perma.cc/B3F6-LVLZ].

draw attention to corruption and civil rights abuses within law enforcement.[64]

The law has engaged in efforts to criminalize doxing when it is used for political purposes, but it has failed to criminalize doxing when used *solely* for malicious purposes (i.e., punching down doxing). In fact, some of the strongest antidoxing regulations protect public figures, while private citizens like Brianna Wu are left without effective remedies.[65] For example, Texas has taken legislative action to make it easier to prosecute people who dox police officers.[66] In addition, federal law applies to doxing incidents that result in economic harm to businesses, such as Internet activist Aaron Swartz's dox of academic articles from the subscription service JSTOR for the purpose of making academic information freely available.[67]

The reason for such different protections under the law is confusing, especially because government transparency is an important principle that some scholars consider equal to individual privacy.[68] Indeed, corporations, government entities, and public figures have a lesser privacy interest than individuals.[69]

3. Internal Regulation: Unmasking Troublemakers

Doxing is also used for "internal regulation" or "self-regulation."[70] Hackers use this doxing category to expose (or "to unmask") the identity of fellow hackers who, for one reason or another, have fallen out of favor with their peers.[71]

For example, members of Anonymous ("Anons"), involved in a campaign against Scientology, doxed fellow Anon, darr, when she "attempt[ed] to push through an unpopular proposal" by "railroad[ing]" the rest of the group.[72] In addition, hackers doxed LulzSec leader-turned-FBI-informant Sabu in an attempt to reveal his identity to the authorities so that

---

64. *Id.*

65. *See, e.g.*, TEX. PENAL CODE ANN. § 38.15(d)(1) (West 2015) (creating a rebuttable presumption that a person is interfering with a peace officer if she intentionally disseminates the home address, home telephone number, or social security number of the officer or a family member of the officer).

66. *Id.*

67. *See* John Schwartz, *Internet Activist, a Creator of RSS, Is Dead at 26, Apparently a Suicide*, N.Y. TIMES (Jan. 12, 2013), http://www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html (describing the life and death of tech pioneer Aaron Swartz, who faced thirty-five years in prison and $1 million in fines for violating federal law in an effort to make JSTOR articles freely accessible) [https://perma.cc/KZ52-H4TB].

68. *See* Martin E. Halstuk et al., *Tipping the Scales: How the U.S. Supreme Court Eviscerated Freedom of Information in Favor of Privacy*, *in* TRANSPARENCY 2.0: DIGITAL DATA AND PRIVACY IN A WIRED WORLD 17, 19–20 (David Cuillier & Charles N. Davis eds., 2014).

69. *See generally* Hustler Magazine, Inc. v. Falwell, 485 U.S. 46 (1988); N.Y. Times Co. v. Sullivan, 376 U.S. 254 (1964); Quin S. Landon, *The First Amendment and Speech-Based Torts: Recalibrating the Balance*, 66 U. MIAMI L. REV. 157 (2011).

70. *See* COLEMAN, *supra* note 25, at 73.

71. *See id.*

72. *Id.*

he would be prosecuted.[73] This type of doxing falls in a gray area between doxing for malicious purposes and doxing for political purposes. While this Note's search for a remedy focuses specifically on punching down doxing, unmasking helps to differentiate the kinds of intent that can underlie an actor's use of doxing.

C. Doctrinal Background

This section discusses two relevant doctrines underlying, influencing, and limiting the possible remedies for punching down doxing: (1) the right to privacy and (2) the First Amendment right to freedom of speech.

1. Right to Privacy

The act of doxing implicates, by necessity, the subject's right to privacy. Privacy is treasured in the United States. In his dissent in *Olmstead v. United States*,[74] Justice Louis Brandeis noted that "the right to be let alone [is] the most comprehensive of rights and the right most valued by civilized [people]."[75]

As technology changes, so do notions of privacy. Historically, privacy cases have asserted two constitutional values: "the individual interest in avoiding disclosure of personal matters" and "the interest in independence in making certain kinds of important decisions."[76] Thus, doxing is uniquely harmful to the right of privacy because "there is no frontier where [one] may go to get a new start. . . . All of our important acts, our setbacks, the accusations made against us go into data banks and are instantly retrievable."[77] Today, our data move about ceaselessly, so "the right to control the way others use the information concerning us" increases in importance as prevailing historical notions of privacy evolve.[78]

However, the right to privacy is not absolute and often runs against freedom of speech and freedom of information.[79] This conflict comes into play when actors dox publicly available information such as home addresses. The interaction of privacy and access to information is not

---

73. Derek Mead, *Sabu Has Been an FBI Informant for Months*, MOTHERBOARD BLOG (Mar. 6, 2012, 10:26 AM), http://motherboard.vice.com/read/months-before-his-arrest-sabu-was-railing-against-doxing-while-snitching-to-the-feds ("Doxing, in the world of modern hacking, is more or less a guaranteed jail sentence.") [https://perma.cc/547Y-3BFG]. Sabu's cooperation resulted in the prosecution of several other Anons. *See* COLEMAN, *supra* note 25, at 391.

74. 277 U.S. 438 (1928).

75. *Id.* at 478 (Brandeis, J., dissenting).

76. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762 (1989) (quoting Whalen v. Roe, 429 U.S. 589, 598–600 (1977)).

77. Sampson v. Murray, 415 U.S. 61, 96 (1974). Although he was discussing computer data storage more generally, Justice William H. Rehnquist's words ring true when applied to the Internet. *See id.*

78. Norberto Nuno Gomes de Andrade, *The Right to Privacy and the Right to Identity in the Age of Ubiquitous Computing*, *in* PERSONAL DATA PRIVACY AND PROTECTION IN A SURVEILLANCE ERA: TECHNOLOGIES AND PRACTICES 19, 22–23 (Christina Akrivopoulou & Athanasios Psygkas eds., 2010).

79. *See* Halstuk et al., *supra* note 68, at 19–20.

simply "a negotiation between the doctrinal principles of each body of law: the presumption of openness that forms the basis of access law versus the expectation of privacy giving rise to informational privacy."[80]

2. The First Amendment

Any approach to providing a legal remedy for doxing victims must comport with the First Amendment. Actors commonly defend themselves by claiming that "they are only exercising their First Amendment right to free speech. And in many cases, an examination of their speech could lead [courts] to concur."[81] Challengers to statutory solutions for doxing could raise two primary arguments: (1) that a statute is void for vagueness and (2) that a statute is overbroad by punishing protected speech.[82]

The First Amendment rests on the underlying principle that "the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable."[83] In addition to protecting spoken and written communication, the First Amendment protects "expressive conduct so long as that conduct 'convey[s] a particularized message' and is likely to be understood in the surrounding circumstances."[84] However, "the [First] Amendment has no application when what is restricted is not protected speech."[85] This subsection explores protected speech and exceptions to First Amendment doctrine that remove certain categories of speech and expressive conduct from constitutional protection.

a. Background

The First Amendment broadly protects communication. "[S]o long as the means are peaceful, the communication need not meet standards of acceptability."[86] Notions of "acceptability" encompass speech that is

80. Charles N. Davis & David Cuillier, *Introduction* to TRANSPARENCY 2.0: DIGITAL DATA AND PRIVACY IN A WIRED WORLD, *supra* note 68, at vii, vii.

81. Michael J. Prout, Assistant Dir. for Judicial Sec., U.S. Marshals Serv., Written Statement Presented to the United States Sentencing Commission Public Hearing on the Court Security Improvement Act of 2007 (Mar. 17, 2009), http://www.ussc.gov/sites/default/files/pdf/amendment-process/public-hearings-and-meetings/20090317/Prout_testimony.pdf [https://perma.cc/6E55-2H4T].

82. Leong & Morando, *supra* note 34, at 132.

83. Texas v. Johnson, 491 U.S. 397, 414 (1989) (collecting cases); *see also* Hustler Magazine, Inc. v. Falwell, 485 U.S. 46, 55 (1988) (rejecting an outrageousness standard for speech because it "runs afoul of our longstanding refusal to allow damages to be awarded because the speech in question may have an adverse emotional impact on the audience"); Members of the City Council v. Taxpayers for Vincent, 466 U.S. 789, 804 (1984); Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 65, 72 (1983); Carey v. Brown, 447 U.S. 455, 462–463 (1980); FCC v. Pacifica Found., 438 U.S. 726, 745–46 (1978) ("[I]t is a central tenet of the First Amendment that the government must remain neutral in the marketplace of ideas."); Young v. Am. Mini Theatres, Inc., 427 U.S. 50, 63–65, 67–68 (1976).

84. Kaahumanu v. Hawaii, 682 F.3d 789, 798 (9th Cir. 2012) (quoting Spence v. Washington, 418 U.S. 405, 409–11 (1974) (per curiam)).

85. Nev. Comm'n on Ethics v. Carrigan, 564 U.S. 117, 121 (2011).

86. Org. for a Better Austin v. Keefe, 402 U.S. 415, 419 (1971).

vulgar, offensive, and disagreeable.[87] For example, "[s]exual expression which is indecent but not obscene is protected by the First Amendment."[88] Of course, broadly protecting vulgar and indecent speech may, to some, create a world filled with "verbal tumult, discord, and even offensive utterance."[89] But this characterization represents a "necessary side effect[] of the broader enduring values which the process of open debate permits us to achieve. That the air may at times seem filled with verbal cacophony is, in this sense not a sign of weakness but of strength."[90]

These broad protections are essential to prevent "empower[ing] a majority to silence dissidents simply as a matter of personal predilections."[91] Moreover, "the fact that society may find speech offensive is not a sufficient reason for suppressing it. If it is the speaker's opinion that gives offense, that consequence is a reason for according it constitutional protection."[92] In addition, First Amendment protection extends beyond traditional speech to encompass expressive conduct[93] and speech via the Internet.[94]

b. The "True Threat" Exception

The First Amendment is not an absolute bar to regulating speech. Certain categories of expression are either "not within the area of constitutionally protected speech"[95] or the "protection of the First Amendment does not extend" to them.[96] The question is whether certain types of harmful speech, such as doxing, can be proscribed without running afoul of the First Amendment.[97] In *Cohen v. California*,[98] the Supreme Court held that the ability to regulate speech depends on a showing that "substantial privacy interests are being invaded in an essentially intolerable manner."[99]

---

87. *Id.*

88. Sable Commc'ns of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989) (finding that prohibiting obscene telephone messages was constitutional and that the denial of adult access to telephone messages that were indecent but not obscene far exceeded that which was necessary to limit access of minors to such messages and did not survive constitutional scrutiny).

89. Cohen v. California, 403 U.S. 15, 24–25 (1971).

90. *Id.* at 25.

91. *Id.* at 21 (reversing a state disturbing the peace conviction for a man who wore a jacket in court that said "fuck the draft").

92. FCC v. Pacifica Found., 438 U.S. 726, 745 (1978).

93. *See, e.g.*, *Cohen*, 403 U.S. at 18.

94. *See, e.g.*, Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1091–93 (W.D. Wash. 2001).

95. R.A.V. v. City of St. Paul, 505 U.S. 377, 383 (1992) (quoting Roth v. United States, 354 U.S. 476, 483 (1957)).

96. *Id.* at 383 (quoting Sable Commc'ns of Cal., Inc. v. FCC, 492 U.S. 115, 124 (1989); Bose Corp. v. Consumers Union of U.S., Inc., 466 U.S. 485, 504 (1984)).

97. *See* Ronald Turner, *On Free, Harmful, and Hateful Speech*, 82 TENN. L. REV. 283, 285 (2015) (discussing the interaction between harmful speech and the First Amendment).

98. 403 U.S. 15 (1971).

99. *Id.* at 21.

The First Amendment does not protect speech or writing that is as an integral part of criminal conduct.[100] The exception most relevant to this Note's effort to find a remedy for doxing is the "true threat" exception.

True threats are not constitutionally protected by the First Amendment.[101] They encompass statements in which the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence against a particular individual or group of individuals.[102] The true threat exception is exemplified by the idea that, "while advocating for violence is considered protected speech, threatening a particular individual with violence is not."[103] However, statements that amount to political hyperbole do not constitute true threats.[104]

Actual intent to carry out the threat is not required for a communication to constitute a true threat.[105] Rather, a prohibition on true threats "protect[s] individuals from the fear of violence" and "from the disruption that fear engenders," in addition to protecting people "from the possibility that the threatened violence will occur."[106] True threats can also include intimidation, when "a speaker directs a threat to a person or group of persons with the intent of placing the victim in fear of bodily harm or death."[107] Importantly, the true threat exception extends to true threats that are posted on a website[108] or communicated over email.[109]

In deciding whether speech constitutes a true threat and is thus unprotected by the First Amendment, courts consider the totality of the circumstances, whether the threat is conditional, and the reaction of the listeners.[110]

---

100. Giboney v. Empire Storage & Ice Co., 336 U.S. 490, 498 (1949); *see also* Commonwealth v. Johnson, 21 N.E.3d 937, 946–47 (Mass. 2014) ("The defendants point to no lawful purpose of their 'communications' that would take them outside of the exception delineated in *Giboney*.").

101. Virginia v. Black, 538 U.S. 343, 359–60 (2003).

102. *See id.*; R.A.V. v. City of St. Paul, 505 U.S. 377, 388 (1992).

103. Marie-Helen Maras, *Unprotected Speech Communicated Via Social Media: What Amounts to a True Threat?*, 19 J. INTERNET L. 3, 3 (2015).

104. Watts v. United States, 394 U.S. 705, 707–08 (1960) (finding that to convict for threatening the President's life, the government must first prove a true threat that is not political hyperbole).

105. *R.A.V.*, 505 U.S. at 383.

106. *Id.* at 408.

107. *Black*, 538 U.S. at 360.

108. *See* United States v. Sutcliffe, 505 F.3d 944, 960–61 (9th Cir. 2007); D.C. v. R.R., 106 Cal. Rptr. 3d 399, 421–22 (Ct. App. 2010); *see also* Novartis Vaccines & Diagnostics, Inc. v. Stop Huntingdon Animal Cruelty USA, Inc., 50 Cal. Rptr. 3d 27, 39 (Ct. App. 2006) (finding that a website maintained by an organization opposed to animal testing was not protected under the First Amendment when the website contained information about a biopharmaceutical company's employees, including home addresses, and made particularized threats of arson against the employees).

109. Abbott v. Maryland, 989 A.2d 795, 826 (Md. Ct. Spec. App. 2010) (finding that an instruction distinguishing a true threat from constitutionally protected speech must be given in a case involving a threat sent by email).

110. United States v. Fullmer, 584 F.3d 132, 154 (3d Cir. 2009). The court found that news posts on an animal rights organization's website fell within First Amendment protection, while posts that "disseminate the personal information of individuals employed by [the animal testers]" are "more problematic" and concluded that electronic

For example, in *Elonis v. United States*,[111] the Supreme Court held that sole reliance on an objective intent standard in assessing true threats would not suffice.[112] In interpreting a federal statute prohibiting threatening interstate communications that lacked a mens rea requirement, the Court noted that the mens rea element would be "satisfied if the defendant transmit[ted] a communication *for the purpose of* issuing a threat or *with knowledge* that the communication [would] be viewed as a threat."[113] The Court, however, did not decide whether a reckless mens rea would suffice.[114]

II. CURRENT APPROACHES TO PROVIDING A REMEDY FOR DOXING ARE INSUFFICIENT

Despite the incredible injuries malicious doxing causes, few legal remedies for subjects exist.[115] This part evaluates whether current federal and state statutory and common law schemes that regulate other forms of doxing and cyberharassment can remedy punching down doxing. Part II.A discusses three current federal statutes and one proposed statute applicable to malicious doxing, and it analyzes the shortcomings of each. Part II.B focuses on state criminal and common law approaches that capture some instances of cyberharassment and explains their ineffectiveness as applied to doxing.

A. Federal Statutory Approaches and Their Limitations

This section discusses three federal statutes relevant to a search for a remedy for malicious doxing: (1) section 230 of the Communications

communications encouraging or describing an illegal act at a specific time, in combination with the other materials, constitute a true threat (in this case, going to burn down an animal tester's house at a certain time). *Id.* at 155l; *see also* Torres v. Clark, No. 1:CV-10-1323, 2012 WL 4484915, at *9 (M.D. Pa. Sept. 27, 2012), *aff'd*, 522 F. App'x 103 (3d Cir. 2013). In *Torres*, the court found a true threat when a prisoner wrote that if a corrections officer "keep[s] acting like he is above policy/law somebody is going to break his jaw is what I assume?!" when he knew that the officer was reading his mail. *Id.* at *3. The prison's dangerous environment meant that threats of violence against corrections officers must be taken seriously. *Id.* at *9. For more on conditional threats constituting true threats, see United States v. Kosma, 951 F.2d 549, 554 n.8 (3d Cir. 1991).

111. 135 S. Ct. 2001 (2015).

112. *See* Maras, *supra* note 103, at 7.

113. Elonis v. United States, 135 S. Ct. 2001, 2004 (2015) (emphasis added). On remand, the Third Circuit upheld Elonis's conviction on the grounds that that the trial court's error (instructing the jury that the negligence standard was sufficient to convict) was harmless. United States v. Elonis, 841 F.3d 589, 601 (3d Cir. 2016). In addition, Elonis's "testimony at trial focused on [the] purpose of his Facebook posts, but never contested that he knew his posts would be viewed as threats." *Id*. at 599. Thus, a jury could have found that Elonis knew the "threatening nature" of his posts, even if the jury believed his testimony. *Id.*

114. *See Elonis*, 135 S. Ct. at 2004.

115. *See* ALICE E. MARWICK & ROSS MILLER, FORDHAM CTR. ON LAW & INFO. POLICY, ONLINE HARASSMENT, DEFAMATION, AND HATEFUL SPEECH: A PRIMER OF THE LEGAL LANDSCAPE 5–6 (2014), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1002&context=clip [https://perma.cc/2ZGG-VNTC].

Decency Act[116] (CDA), (2) the Interstate Communications Statute,[117] and (3) the Interstate Stalking statute.[118] This section also examines a current bill. Further, this section addresses the weaknesses of each federal approach and explains why none suffices to create an appropriate remedy for doxing.

1. The Communications Decency Act

Part 2.A.1.a provides an overview of the CDA, explaining the protections it affords to online service providers by shielding them from liability. Part 2.A.2.b then discusses the statute's limitations as applied to doxing.

a. Overview of the Statute

The CDA applies to malicious doxing by creating a liability shield for online services and thus removing a potential pathway to a doxing remedy. The CDA regulates obscene content on the Internet such as child pornography and other indecent content accessible to children.[119] However, section 230 of the CDA provides that 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."[120] Interactive computer service providers include, among other things, search engines,[121] social media networks,[122] hosts of online business reviews,[123] online vendors,[124] and operators of sites that have message boards.[125]

The CDA's "Good Samaritan" provision limits liability for these online services by separating the services (e.g., Twitter) from individual speakers or posters who use them (e.g., Twitter users). Using the Gamergate example discussed in Part I.B.1, Twitter could not be held liable under the CDA for a Twitter user harassing and doxing Brianna Wu.

In addition to limiting liability for hosting constitutionally protected but "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" material,[126] the CDA also limits liability for speech that is not constitutionally protected.[127] Accordingly, the CDA operates as a liability shield, eliminating the possibility of a remedy by

116. 47 U.S.C. § 230 (2012).
117. 18 U.S.C. § 875.
118. *Id.* § 2261A.
119. 47 U.S.C. § 223(a).
120. *Id.* § 230(c)(1).
121. Stayart v. Yahoo! Inc., 651 F. Supp. 2d 873, 873 (E.D. Wis. 2009).
122. Caraccioli v. Facebook, Inc., 167 F. Supp. 3d 1056, 1066 (N.D. Cal. 2016).
123. Kimzey v. Yelp Inc., No. C13-1734RAJ, 2014 WL 1805551 (W.D. Wash. May 7, 2014).
124. Joseph v. Amazon.com, Inc., 46 F. Supp. 3d 1095, 1105–07 (W.D. Wash. 2014).
125. DiMeo v. Max, 248 F. App'x 280, 282 (3d Cir. 2007).
126. 47 U.S.C. § 230(c)(2)(A) (2012).
127. *See, e.g.*, GoDaddy.com, LLC v. Toups, 429 S.W.3d 752 (Tex. App. 2014) (finding that the purportedly unconstitutional nature of revenge porn images posted to websites without the consent of the subjects did not affect the court's determination of whether the interactive computer service provider that hosted the websites was entitled to immunity under the CDA).

limiting the liability of Internet service providers that host doxed content, regardless of whether that content is constitutionally protected.

The CDA has two parallel goals: (1) "to promote the free exchange of information and ideas over the Internet" and (2) "to encourage voluntary monitoring for offensive or obscene material."[128] These goals, together with the protections provided by the CDA, have caused online civil liberties advocates to hail the Act as "the most important law protecting internet speech."[129]

The Good Samaritan provision was also "added to the CDA as part of the CDA's overall goal to 'clean up' the Internet from obscene materials," and it limits liability for online services to "enable filtering or blocking . . . to spur the advancement of content filtering technologies."[130] An early decision addressing the provision found that an "important purpose of § 230 was to encourage service providers to self-regulate the dissemination of offensive material over their services," thereby minimizing the necessity of state regulation of Internet speech.[131]

b. Limitations of the Statute as Applied to Doxing

Because of section 230, applying the CDA to punching down doxing would shield an entire class of possible defendants—service providers—from liability for doxing. In applying the CDA, "[c]ourts have roundly immunized site operators from liability even though they knew or should have known that user-generated content contained defamation, privacy invasions, intentional infliction of emotional distress, and civil rights violations."[132] The immunity provides "little incentive for [services] to self-regulate the appropriateness of the content posted there, leaving sites as blank canvases readily available for the actual parties to directly furnish inappropriate material online."[133]

For example, in *Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc.*,[134] the Seventh Circuit found Craigslist immune from liability under the CDA for users' discriminatory housing advertisements, which violated the Fair Housing Act.[135] Thus, the CDA

128. Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1099–100 (9th Cir. 2009) (quoting Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1122 (9th Cir. 2003)).

129. *CDA 230: The Most Important Law Protecting Internet Speech*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/cda230 (last visited Mar. 25, 2017) [https://perma.cc/4RCR-TXAX].

130. Arthur Chu, *Mr. Obama, Tear Down This Liability Shield*, TECHCRUNCH (Sept. 29, 2015), https://techcrunch.com/2015/09/29/mr-obama-tear-down-this-liability-shield/ [https://perma.cc/KD8M-VT7L].

131. Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).

132. CITRON, *supra* note 16, at 171.

133. Quon, *supra* note 45, at 590.

134. 519 F.3d 666 (7th Cir. 2008).

135. *Id.* at 670.

limits the remedies available to doxing subjects and leaves them without redress for their injuries.[136]

Scholars have proposed various amendments to the CDA.[137] One proposal calls for a take-down provision that "would work much like the safe harbor under section 512 of the Digital Millennium Copyright Act ('DMCA'), which protects [services] who inadvertently host materials that infringe intellectual property rights."[138] This proposal would require that services take down offensive content once they are notified—that content could include doxes. Congress could assign the Federal Communications Commission to create guidelines for companies to help determine which types of communications should be taken down.[139]

Another proposal would remove the safe harbor provision for sites that "encourage cyber stalking or nonconsensual pornography and make money from its removal *or* that principally host cyber stalking or nonconsensual pornography."[140] Yet another would create a unique cause of action for injunctive relief available to subjects whose personal information is posted online.[141] In Spain, citizens can sue to have sensitive information pertaining to them removed from the Internet under the Spanish Data Protection Authority.[142] This strategy could be applied to doxing. However, this so-called "right to be forgotten" in the European Union applies only when information is "inaccurate, inadequate, irrelevant, or excessive," and the right is balanced against fundamental rights like the freedom of expression.[143] Therefore, this carve out, if included, might not capture doxing after all. In addition, an amendment to section 230's safe harbor provision would need to cover actions outside of defamation, or else doxing could not be addressed.

2. The Interstate Communications Statute

Part II.A.2.a. provides an overview of the Interstate Communications Statute, 18 U.S.C. § 875. Part II.A.2.b discusses limitations of the statute as applied to doxing and provides reasons why it fails to serve as an effective solution.

---

136. *See* Alison Virginia King, *Constitutionality of Cyberbullying Laws: Keeping the Online Playground Safe for Both Teens and Free Speech*, 63 VAND. L. REV. 845, 878 (2010).

137. *See, e.g.*, JOEL REIDENBERG ET AL., FORDHAM CTR. ON LAW & INFO. POLICY, SECTION 230 OF THE COMMUNICATIONS DECENCY ACT: A SURVEY OF THE LEGAL LITERATURE AND REFORM PROPOSALS 47–52 (2012), https://www.fordham.edu/download/downloads/id/1825/clip_section_230_of_the_communications_decency_act_report.pdf [https://perma.cc/TW4A-HAFG].

138. *See* King, *supra* note 136, at 878 & n.209.

139. *Id.* at 878.

140. *See* CITRON, *supra* note 16, at 177.

141. Konstantinos K. Stylianou, *Hasta La Vista Privacy, or How Technology Terminated Privacy*, *in* PERSONAL DATA PRIVACY AND PROTECTION IN A SURVEILLANCE ERA: TECHNOLOGIES AND PRACTICES, *supra* note 78, at 44, 51.

142. *Id.*

143. EUROPEAN COMM'N, FACTSHEET ON THE "RIGHT TO BE FORGOTTEN" RULING (*C-131/12*) (2014), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf [https://perma.cc/BJ6X-PVMB].

a. Overview of the Statute

The Interstate Communications Statute—specifically § 875(c)—criminalizes the Internet transmission[144] of "any communication containing any threat to kidnap any person or any threat to injure the person of another."[145] Federal prosecutors could use § 875(c) to prosecute actors who dox in combination with administering threats. Indeed, this statute could apply to Gamergate actors who harassed, threatened, and doxed Wu and others.

Under § 875(c), the threatened party need not actually receive the threat.[146] In addition, this statute does not require the threatener to have actually intended to carry out the threat if "the threat on its face and in the circumstances in which it is made is so unequivocal, unconditional, immediate and specific as to the person threatened, as to convey a gravity of purpose and imminent prospect of execution."[147] In *Elonis*, the Supreme Court held that a purposeful or knowing mens rea is sufficient to establish culpability under § 875(c); however, the Court left it to the lower courts to determine whether recklessness would also suffice.[148]

b. Shortcomings of the Interstate Communications Statute

While § 875(c) comes close to covering some instances of doxing, it fails to provide a completely effective solution for three reasons. First, the actions the actor undertakes must constitute a threat to kidnap or injure the subject.[149] If the speech is a "true threat," it falls under the true threat exception to the First Amendment and thus can be regulated.[150] In many instances of doxing, an actor "may never convey an explicit threat to kidnap or injure his or her victim, yet the victim could still have good reason to be terrified."[151] Thus, it is unlikely that a dox will contain a specific, explicit threat. However, courts' interpretations of a similar statute can shed some light on how § 875 could best be construed to capture malicious doxing, even when it is not accompanied by an additional specific threat. For

144. 18 U.S.C. § 875(c) (2012). The statute's language criminalizes interstate transmission; however, proving Internet transmission alone is sufficient to prove transmission through interstate commerce for the purposes of this statute. *Id.*

145. *Id.*

146. United States v. Kistler, 558 F. Supp. 2d 655, 656 n.2 (W.D. Va. 2008).

147. United States v. Kelner, 534 F.2d 1020, 1027 (2d Cir. 1976) (finding that no specific intent is required when "the threat itself may affront such important social interests that it is punishable absent proof of a specific intent to carry it into action").

148. Elonis v. United States, 135 S. Ct. 2001, 2004 (2015). On remand, the Third Circuit did not reach whether recklessness specifically sufficed, but it held that "Section 875(c) contains both a subjective and objective component, and the Government must satisfy both in order to convict a defendant under the statute." United States v. Elonis, 841 F.3d 589, 596, 601 (3d Cir. 2016).

149. *See supra* note 144 and accompanying text.

150. *See Elonis*, 135 S. Ct. at 2004; *see also supra* Part I.C.2.a.

151. *Federal Criminal Statutes*, U.N.C. CHAPEL HILL: CYBERSTALKING, http://cyberstalking.web.unc.edu/federal-criminal-statutes/ (last visited Mar. 25, 2017) [https://perma.cc/8Y9T-9F69].

example, the Freedom of Access to Clinic Entrances Act (FACE) criminalizes threats made to providers of reproductive health services.[152] In *Planned Parenthood v. American Coalition of Life Activists*,[153] the Ninth Circuit held that the doxing of the names and addresses of health providers on "wanted"-style posters constituted a true threat without an additional, specific threat of violence.[154] The court found that the defendant "was aware that a 'wanted'-type poster would likely be interpreted as a serious threat of death or bodily harm by a doctor in the reproductive health services community who was identified on one, given the previous pattern of 'WANTED' posters identifying a specific physician followed by that physician's murder."[155]

Accordingly, one effective approach to doxing could be to find that a dox of names and addresses online is a true threat without an additional, specific threat of violence. However, the *Planned Parenthood* Court's approach required the homicide of another doctor to happen before finding a true threat.[156] This logic lends weight to Gamergate victim Zoe Quinn's fears "that what it's going to take to stop [the doxing and harassment of victims without a remedy] is the death of one of the women who's been targeted."[157]

The second drawback of § 875(c) is the possibility that lower federal courts will employ the Supreme Court's "purposeful or knowing mens rea" standard in *Elonis* to determine true threats under the statute without also adopting the recklessness standard, making it harder to prosecute threats.[158] The first standard—purposefulness—requires "a subjective intent to threaten," which is similar to regular criminal intent.[159] Under the Model Penal Code, this standard requires proof that a defendant "consciously wants to cause a certain result."[160] "At trial, the prosecution would rely on statements made by the defendant to cohorts, and assembling different pieces of evidence, in order to convince the fact finder that the defendant possessed specific intent" to threaten the subject.[161]

The second standard—knowledge—requires showing the defendant's knowledge that the communication would be viewed as a threat.[162] The

152. 18 U.S.C. § 248 (2012). FACE creates a private right of action against anyone who by "threat of force . . . intentionally . . . intimidates . . . any person because that person is or has been . . . providing reproductive health services." *Id.* § 248(a)(1); *see id.* § 248(c)(1)(A).

153. 290 F.3d 1058 (9th Cir. 2002).

154. *Id.* at 1063.

155. *Id.*

156. *Id.*

157. Stuart, *supra* note 55.

158. *See* Elonis v. United States, 135 S. Ct. 2001, 2004 (2015) ("Section 875(c)'s mental state requirement is satisfied if the defendant transmits a communication for the purpose of issuing a threat or with knowledge that the communication will be viewed as a threat. The Court declines to address whether a mental state of recklessness would also suffice.").

159. Jing Xun Quek, Elonis v. United States*: The Next Twelve Years*, 31 BERKELEY TECH. L.J. 1109, 1126 (2016).

160. *See id.* at 1116.

161. *Id.* at 1126.

162. *See id.*

Model Penal Code's definition of "knowingly" requires proof that a defendant "is practically certain that his conduct will cause [the intended] result."[163] These higher standards could risk undercriminalizing threatening communications—a dangerous prospect when the nature of social media exacerbates the dangers inherent in true threats.[164]

However, a recklessness standard would provide greater protection for doxing subjects while still comporting with the true threat doctrine.[165] Recklessness contemplates the subject's objective interpretation of the threat along with the subjective intent of the actor. This is critical because the National Network to End Domestic Violence argues that "victims are often the best assessors of the risk that the threats of violence they face will be carried out."[166] The objective context of a message would help prosecutors and law enforcement to understand the meaning and implications of that message.[167]

The third issue with § 875(c) is that many law enforcement officers are simply unaware that the statute exists and could be used to prosecute doxing.[168] In fact, one subject found that seeking legal recourse "only continually put [her] in harm's way."[169] For example, after she was doxed, Brianna Wu called the police.[170] The FBI assigned a special agent to her case, which was then reassigned to the state attorney general's office, which has not yet pursued charges.[171] Because of her high-profile case, Wu believes that law enforcement "[has] every reason to want to solve this crime, but at the same time nothing has happened, even giving them as much information as [she] ha[s]."[172] Wu and her husband explained to the FBI agent that they "feel like [they] are sending emails into the void" and that "[they] do not have any faith that the FBI is interested in helping [their] family."[173] Accordingly, any adequate remedy for doxing will provide for the training of law enforcement officers so that they can better help doxing victims who are in danger.

---

163. *Id.* at 1116.

164. *See id.* at 1135; *see also supra* Part I.A.1.

165. *See infra* Part III.A.

166. Brief of Amici Curiae the National Network to End Domestic Violence et al. in Support of Respondent at 19 n.34, Elonis v. United States, 135 S. Ct. 2001 (2015) (No. 13-983); *see also* Leong & Morando, *supra* note 34.

167. Jessica K. Formichella, *A Reckless Guessing Game: Online Threats Against Women in the Aftermath of* Elonis v. United States, 41 SETON HALL LEGIS. J. (forthcoming 2017).

168. Nick Visser, *Woman Targeted in 'GamerGate' Harassment Drops Charges*, HUFFINGTON POST (Feb. 11, 2016, 1:46 AM), http://www.huffingtonpost.com/entry/zoe-quinn-gamergate-charges_us_56bc1d13e4b0b40245c56102 [https://perma.cc/A79F-NGXM].

169. *Id.*

170. Merlan, *supra* note 6.

171. Dewey, *supra* note 1.

172. Merlan, *supra* note 6.

173. Dewey, *supra* note 1.

3. The Interstate Stalking Statute

Part II.A.3.a. provides an overview of the Interstate Stalking Statute, 18 U.S.C. § 2261A, including a brief discussion of its 2013 amendment. Part II.A.3.b further discusses the limitations of the Interstate Stalking Statute as applied to doxing and law enforcement's unwillingness to enforce the statute.

a. Overview of the Statute

Section 2261A(2) of the Interstate Stalking Statute prohibits the use of "any interactive computer service" in a "course of conduct" that places a person in reasonable fear of death or serious bodily injury or "causes substantial emotional distress to a person."[174] Whether this statute could be used to prosecute malicious doxing depends on whether the dox constitutes a "course of conduct." For example, to prosecute the Gamergate actor under the statute in Brianna Wu's case, the actor's tweets must constitute a "course of conduct." The statute requires "intent to kill, injure, harass, or place under surveillance with intent to kill, injure, harass, or intimidate another person."[175]

Congress enacted the statute in 1996 as part of the Violence Against Women Act (VAWA), primarily to combat in-person stalking resulting in physical harm to victims.[176] However, "[w]ith the proliferation of cheap technology that allows instantaneous tracking and monitoring of victims, the frequency of cyberstalking has risen dramatically."[177] Accordingly, Congress amended VAWA in 2013 to include explicit provisions for cyberstalking.[178]

A "course of conduct" is an element of any offense under § 2261A(2) and means "a pattern of conduct composed of two or more acts."[179] In 2015, the U.S. District Court for the District of Delaware convicted three defendants on charges of cyberstalking that resulted in a death.[180] They "conducted a campaign to surveil and harass" the victim, Christine Belford, one of the defendants' ex-wife.[181] Over four years, the defendants "posted accusations against the victim online, sent accusations against Belford to the school that one of the children attended and to Belford's church, and

174. 18 U.S.C. § 2261A(2)(A)–(B) (2012).

175. *Id.* § 2261A(2).

176. *See* Melvin Huang, Note, *Keeping Stalkers at Bay in Texas*, 15 TEX. J. ON C.L. & C.R. 53, 59–60 (2009) (discussing the 1990s movement toward criminalizing stalking following the murder of actress Rebecca Schaeffer by an obsessed fan who stalked her for two years).

177. *Id.* at 56–57 ("[C]yberstalking has replaced traditional methods of stalking and harassment." (quoting U.S. DEP'T OF JUSTICE, STALKING AND DOMESTIC VIOLENCE: REPORT TO CONGRESS 5 (2001)).

178. *See* STALKING RES. CTR., NAT'L CTR. FOR VICTIMS OF CRIME, SUMMARY OF CHANGES FROM VAWA 2013 RELATED TO STALKING (2013), http://www.victimsofcrime.org/docs/src/vawa-2013-and-stalking.pdf?sfvrsn=2 [https://perma.cc/WTS2-RBHW].

179. United States v. Bell, 303 F.3d 1187, 1192 (9th Cir. 2002).

180. *See* United States v. Matusiewicz, 165 F. Supp. 3d 166, 167 (D. Del. 2015).

181. *Id.*

solicited their friends' assistance in visiting Belford's home to monitor Belford."[182]

This case is the first in which defendants "were convicted of cyberstalking resulting in [a] death."[183] It also demonstrates the high bar necessary to prove a "course of conduct" under the statute.

b. Limitations to the Statute's Application to Doxing

The Interstate Stalking Statute could be an effective tool to combat some instances of doxing, but it is underinclusive because of its "course of conduct" requirement. Additionally, this statute faces the same resource limitation problems as the Interstate Communications Statute.

Section 2261A(2) applies where an actor uses a computer within a "course of conduct" that places a person in reasonable fear of death or serious bodily harm or "causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person."[184] Limitations to this statute's application to doxing exist because actors often work in concert with other actors in a cybermob.[185] Countless threads work together with "one poster starting the abuse and others piling on."[186] If each actor "was responsible for only one or two isolated posts," no single person could likely be held responsible for the "course of conduct" under § 2261A(2).[187]

According to Professor Danielle Keats Citron, the Interstate Stalking Statute is "very helpful" when federal law enforcement agencies enforce it.[188] However, she argues that officers often say, "We're in the business of worrying about murder and terrorism, we don't enforce cyberstalking laws."[189] Meanwhile, officers spend the majority of their time and resources investigating drug crimes and larceny, so it is untrue that federal law enforcement is too busy investigating terrorism and murder—"[t]he statistics belie that."[190] Indeed, federal prosecutors seldom apply the statute to cyberharassment cases.[191] Whereas prosecutors used § 2261A ten times

182. *Id.* It is unclear whether any of the defendants actually doxed Belford, but the opinion indicates that the defendants encouraged others to harass her at her home. *Id.*

183. Press Release, U.S. Att'y's Office, D. Del., Three Family Members Receive Life Sentences for Courthouse Murder Conspiracy (Feb. 19, 2016), https://www.justice.gov/opa/pr/three-family-members-receive-life-sentences-courthouse-murder-conspiracy [https://perma.cc/JL2H-PL6M].

184. *See supra* Part II.A.3.

185. *See* CITRON, *supra* note 16, at 136.

186. *Id.*

187. *Id.* at 136–37.

188. Merlan, *supra* note 6.

189. *Id.*

190. *Id.*

191. *See* CITRON, *supra* note 16, at 85.

from 2010 to 2013,[192] an estimated 3.3 million people age eighteen or older were victims of stalking in a single year.[193]

4. Proposed Legislation

U.S. Representative Katherine Clark, who represents the district where Brianna Wu and other doxing subjects live, has proposed several pieces of legislation that would provide some relief to doxing victims. In June 2015, Representative Clark proposed the Prioritizing Online Threat Enforcement Act of 2015, which calls upon the U.S. Attorney General to ensure that at least ten additional FBI agents support the Criminal Division of the Department of Justice in the investigation and coordination of cybercrimes against individuals.[194] In March 2016, Representative Clark introduced the Cybercrime Enforcement Training Assistance Act of 2016, directing the Department of Justice to award grants to state and local governments to prevent, enforce, and prosecute cybercrimes against individuals.[195]

Both bills would provide important support to doxing subjects. The first would address some of the systematic bars to prosecution under federal statutes by assigning more officers to investigate cybercrimes. The second would alleviate some of the concerns addressed in Part II.B by making officers aware of doxing by increasing training at the state and local level.[196]

The House of Representatives referred the Cybercrime Enforcement Training Assistance Act to the House Committee on the Judiciary and then to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.[197] The Prioritizing Online Threat Enforcement Act followed the same path to committee as its successor.[198] It does not have any Republican supporters and is not expected to make it past the subcommittee stage.[199]

B. State Approaches and Their Limitations

This section discusses different ways state legislatures have addressed cyberharassment and how, if at all, these approaches reach doxing. Part

192. *See id.* (finding only ten instances of prosecutorial use of § 2261A from 2010 to 2013).

193. *See* SHANNAN CATALANO, U.S. DEP'T OF JUSTICE, STALKING VICTIMS IN THE UNITED STATES—REVISED (2012), https://www.bjs.gov/content/pub/pdf/svus_rev.pdf [https://perma.cc/2444-MF26].

194. H.R. 2602, 114th Cong. (2016).

195. H.R. 4740, 114th Cong. (2016).

196. *See* discussion *infra* Part II.B.

197. *All Actions: H.R. 4740—Cybercrime Enforcement Training Assistance Act of 2016*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/4740/all-actions (last visited Mar. 25, 2017) [https://perma.cc/N4G8-ZVVE].

198. *All Actions: H.R. 2602—Prioritizing Online Threat Enforcement Act of 2015*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/2602/all-actions (last visited Mar. 25, 2017) [https://perma.cc/7CFN-6G7D].

199. Dewey, *supra* note 1.

II.B.1 covers criminal approaches, and Part II.B.2 covers state common law doctrines that could provide relief to doxing subjects.

1. Criminal: Cyberstalking and Criminal Harassment

Most states, to some extent, have criminalized cyberstalking or have applied criminal harassment statutes to online activity.[200] This subsection discusses state criminal laws that regulate cyberstalking and further discusses the shortcomings with this approach.

a. Overview of State Criminal Statutes Regulating Doxing

Data on the enforcement of cyberstalking and harassment statutes are hard to find because most states do not collect such data.[201] Anecdotal evidence from several states sheds some light on the strengths of state criminal law as an effective remedy for doxing.

For example, in *Commonwealth v. Johnson*,[202] two neighbors were in a dispute over a property.[203] Out of revenge, the defendant posted a false Craigslist ad for free golf carts with the name, address, and phone number of his neighbor, constituting an instance of punching down doxing.[204] Thirty to forty people showed up at the subject's home.[205] Then the defendant posted a false ad for an inexpensive motorcycle with a request to call the neighbor's cell phone after 10:00 p.m.[206] The calls continued for months, up to twenty calls every ten minutes.[207]

Massachusetts charged the defendant with conspiracy and criminal harassment.[208] The Massachusetts Supreme Court found that the criminal harassment statute did not proscribe free speech, because it is "directed at a course of conduct, rather than speech, 'and the conduct it proscribes is not necessarily associated with speech.'"[209] The statute specifically criminalizes "a knowing pattern of conduct . . . or series of acts . . . directed at a specific person, which seriously alarms that person and would cause a reasonable person to suffer substantial emotional distress."[210]

When a statute "proscribes harassing and intimidating conduct, the statute is not facially invalid under the First Amendment."[211] In addition, a

200. *See* CITRON, *supra* note 16, at 104. For a discussion of how state legislatures have approached codifying cyberbullying (cyberharassment by and against school-age children), see Matthew Fenn, Note, *A Web of Liability: Does New Cyberbullying Legislation Put Public Schools in a Sticky Situation?*, 81 FORDHAM L. REV. 2729, 2753–55 (2013).

201. *See* CITRON, *supra* note 16, at 89.

202. 21 N.E.3d 937 (Mass. 2014).

203. *See id.* at 941.

204. *See id.* at 941–42.

205. *See id.* at 942.

206. *See id.*

207. *See id.*

208. *See id.* at 943.

209. *Id.* at 945 (quoting United States v. Petrovic, 701 F.3d 849, 856 (8th Cir. 2012)).

210. *Id.* at 944–45.

211. United States v. Osinger, 753 F.3d 939, 944 (9th Cir. 2014).

statute can contain adequate safeguards to prevent its application to protected speech.[212]

Moreover, the court found that "[t]he defendants cannot launder their harassment of the [victims] through the Internet to escape liability."[213] The Craigslist posts were not protected because they were "the equivalent of the defendants recruiting others to harass the victims and the victims alone."[214] In all, the Massachusetts criminal harassment statute provided an effective remedy for a specific doxing subject.

Several other states have effective criminal laws that can be used to prosecute doxing. Maryland Criminal Code section 3-803 prohibits an intentional, malicious course of conduct that constitutes harassment, as long as the actor has received a reasonable warning or request to stop by or on behalf of the subject.[215]

In addition, Utah Representative David E. Lifferth has introduced House Bill 225, which modifies the existing criminal code to include cybercrimes such as doxing, swatting, and denial of service attacks.[216] The doxing provision of House Bill 225 prohibits the publication of personal identifying information, including name and home address.[217] If constitutional, this bill is an example of a state criminal statute that would provide specific support to doxing subjects.

b. Limitations on the State's Statutory Approach

The overarching problem facing the state statutory approach is the lack of police awareness, training, care, and resources to help enforce and protect because "even the most effectively drafted stalking and harassment laws cannot do much if they are not enforced."[218] Specifically, victims report that officers tend to lack awareness of the problems of cyberharassment and doxing.[219] When one journalist reported an online rape threat to police, the responding officer asked her, "Why would anyone bother to do something like that?" and declined to file a report.[220] "That [her] stalker had said that

212. *See* CITRON, *supra* note 16, at 199–200.
213. *Johnson*, 21 N.E.3d at 948.
214. *Id.*
215. MD. CODE ANN., CRIM. LAW § 3-803 (West 2011).
216. Eugene Volokh, *Utah 'Anti-Doxxing' Bill Would Outlaw Mentioning a Person's Name Online 'With Intent to Offend,'* WASH. POST (Feb. 8, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/08/utah-anti-doxxing-bill-would-outlaw-mentioning-a-persons-name-online-with-intent-to-offend [https://perma.cc/GE86-62KK].
217. H.B. 225, 61st Leg., Gen. Sess. (Utah 2016) (cybercrime statute amendments).
218. CITRON, *supra* note 16, at 105; *see also* Merlan, *supra* note 6 (noting that Citron argues that the biggest problem at the local level is the "lack of technical skills and training for law enforcement officers").
219. CITRON, *supra* note 16, at 88.
220. Amanda Hess, *Why Women Aren't Welcome on the Internet*, PAC. STANDARD (Jan. 6, 2014), https://psmag.com/why-women-aren-t-welcome-on-the-internet-aa21fdbc8d6#.whlavj6fd [https://perma.cc/L4CR-LKAY].

he lived in [her] state, and had plans to seek [her] out at home, was dismissed as just another online ruse."[221]

The practical implications of protecting a subject from an online threat also indicate the difficulty that law enforcement officers face in providing relief. Many harassers are (at least initially) anonymous, and IP addresses can be difficult to trace. As a result, officers sometimes report that they believe they cannot offer assistance if the actor is outside the state or locality.[222] Another journalist who was doxed received an onslaught of harassing messages and threats followed by an inundation of takeout orders sent to her old apartment.[223] When she went to the police to file a report, the officer asked her, "[D]o we know where they physically are? We need physical locations" and declined to file a report.[224] Ultimately, "[t]he advice that police give to victims is to stay offline."[225]

The difficulty of pinpointing the location of an actor highlights the importance of protecting doxing subjects. While the actor's location may be unknown, the location of the threatened attack becomes clear the moment the actor doxes the subject.

Additional limitations apply to specific state statutes. For example, in Massachusetts, the efficacy of the criminal harassment statute is limited by the definition of a "course of conduct."[226] If an actor doxes a subject once, causing extreme emotional distress, this action most likely would not constitute a "course of conduct" and thus cannot be prosecuted under the state criminal harassment statute. Further, many individual actors acting alone would not fall within the meaning of "course of conduct" under a Massachusetts-like statute.[227] Another issue is that the proscribed activity is conduct, not language. In Maryland, the criminal harassment statute requires the victim to intercede and provide a "reasonable warning" to the harasser.[228]

More generally, state laws punish "credible threats of violence."[229] Only a few states "prohibit harassment communicated directly or indirectly, on- or offline."[230] Accordingly, only a few state statutes currently reach subjects who are bullied into silence where those subjects do not feel

221. *Id.*
222. *See* Merlan, *supra* note 6.
223. *See id.*
224. *Id.*
225. CITRON, *supra* note 16, at 84. This is an unacceptable solution. The state argues that it cannot regulate malicious doxing because it is protected by freedom of speech. The state then suggests that doxing subjects avoid the Internet—effectively silencing them. This argument privileges the malicious speech of doxing actors over the speech of subjects and approaches the viewpoint discrimination doctrine under the First Amendment. *See* R.A.V. v. City of St. Paul, 505 U.S. 377, 387 (1992).
226. CITRON, *supra* note 16, at 131.
227. *See* MASS. GEN. LAWS ch. 265, § 43A(a) (2010).
228. MD. CODE ANN., CRIM. LAW § 3-803 (West 2011).
229. CITRON, *supra* note 16, at 123 (citing Holcomb v. Virginia, 709 S.E.2d 711, 716 (Va. Ct. App. 2011) (finding that public threats posted to a MySpace page can support a conviction under the Virginia threat statute, where the defendants proclaimed that he "just had to stab" the victim and "slit [her] neck into a fountain drink" (alteration in original))).
230. *Id.* at 124.

"tangible, sustained, and immediate fear" of an "unequivocal, unconditional, and specific" threat.[231] If any of these exacting elements is not met in a given scenario, current state criminal law cannot provide a remedy for that doxing subject. Accordingly, current state criminal approaches to doxing fall short of providing an effective legal remedy.

2. Common Law: Defamation, Harassment, and IIED

Common law approaches can provide a remedy for doxing. This subsection briefly discusses three different common law torts that can apply to doxing: defamation, harassment, and intentional infliction of emotional distress (IIED).

a. Overview of Common Law Approaches

Tort law can cover some instances of doxing. In many ways it is an appealing approach because of its "flexible dynamic structure," which "permit[s] technological innovation and change while controlling undesirable behavior."[232] Culture and time influence societal expectations and shared beliefs on privacy standards, so the judiciary's ability to make case-by-case determinations that incorporate common beliefs is critical to finding an effective solution for malicious doxing.[233]

Some states recognize a cause of action for defamation that could apply to doxing.[234] In addition, harassment claims can provide some redress for doxing subjects,[235] as can the tort of intentionally or recklessly causing severe emotional distress with extreme and outrageous conduct. This standard sets a high bar for conduct, but "[h]umiliating, threatening, and persistent online cruelty amounts to 'extreme and outrageous' activity because it falls outside the norms of decency."[236]

b. Limitations to Common Law Approaches

The overarching issue with the state common law approach is that it puts the burden of enforcement on the doxing subject. The cost of a lawsuit against a doxing actor is estimated at $10,000 to $60,000 and 500 hours of labor.[237] The subject would bear the entirety of these costs.

---

231. *Id.* at 123.

232. Natalie L. Regoli, Note, *A Tort for Prying E-Eyes*, 2001 U. ILL. J.L. TECH. & POL'Y 267, 277.

233. *Id.*

234. *See, e.g.*, *State Law: Defamation*, DIGITAL MEDIA L. PROJECT, http://www.dmlp.org/legal-guide/state-law-defamation (last visited Mar. 25, 2017) [https://perma.cc/438M-Z4SU].

235. *See* CITRON, *supra* note 16, at 121.

236. *Id.* (quoting Benjamin C. Zipurksy, Snyder v. Phelps, *Outrageousness and the Open Texture of Tort Law*, 60 DEPAUL L. REV. 473 (2011)).

237. Jennifer T. Criss, Assoc., Drinker Biddle & Reath LLP, Remarks at the American Bar Association Program on Doxing, Swatting, Trolls, and SJWs: Harassment and Gender Discrimination on Social Media Platforms (Nov. 8, 2016) (on file with the *Fordham Law Review*).

Additional drawbacks include cause of action, scope, and high standards. For example, defamation does not capture instances of doxing when the information published is true, like a home address. In fact, even "[w]hen people are lied about, they typically expect that some legal recourse will be available, but are often sorely disappointed."[238]

In addition, the "extreme and outrageous conduct" standard required for a prima facie case of IIED is a high standard that restricts recovery for extreme emotional distress more than recovery for physical harm.[239] A one-time tweet of a subject's contact information likely would not rise to the high bar set in IIED. For these reasons, the state common law approach is an imperfect remedy for doxing subjects.

III. A BLENDED SOLUTION: PROPOSING A REMEDY WITH STATE AND FEDERAL STATUTORY ELEMENTS

As discussed in Part II, neither state nor federal law provides a consistent approach to deal with doxing, resulting in severe harm to doxing subjects.[240] While many types of online harassment—such as impersonation, revenge pornography, and defamation—cause harm, doxing puts victims in critical, physical danger. Doxing is a tool that moves purely online harassment into the physical realm.[241] Even though doxed information can be publicly available, people should have the right to control their contact information to keep themselves free from harassment, threats, and living in fear.[242] In addition, the Internet provides a platform to amplify public information and to weaponize it.[243] Accordingly, the best solution to the lack of a doxing remedy involves (1) the widespread adoption by lower federal courts of a recklessness standard for the Interstate Communications Statute to encourage further enforcement and (2) the adoption or amendment of state criminal laws criminalizing malicious doxing under the true threat exception to the First Amendment. To support the adoption of state criminal laws, Congress should pass federal legislation providing funding for state and local law enforcement to train officers to better enforce state cyberharassment law.

A. Lower Federal Courts Should Adopt a Recklessness Standard for the Interstate Communications Statute

As discussed in Part II, the Interstate Communications Statute can be an effective tool for prosecuting doxing;[244] however, the statute has some

238. Ann Bartow, *Internet Defamation as Profit Center: The Monetization of Online Harassment*, 32 HARV. J.L. & GENDER 383, 415 (2009).

239. *See* John J. Kircher, *The Four Faces of Tort Law: Liability for Emotional Harm*, 90 MARQ. L. REV. 789, 837 (2007).

240. *See supra* Part II.A–B.

241. *See supra* notes 28–39 and accompanying text.

242. *See supra* Part II.B.2.

243. *See supra* notes 28–39 and accompanying text.

244. *See supra* Part II.A.2.a.

limitations.[245] To overcome these limitations, the lower federal courts should adopt a recklessness standard for the statute's mens rea.[246]

The Supreme Court has made clear that speech can rise to a true threat through a showing that the speaker purposefully or knowingly intended to threaten the subject.[247] However, recklessness will enable prosecutors to look at the objective effect of the speech and its effect on the subject.[248] Analysis of the totality of the circumstances, which a recklessness standard would provide, will give dimension to online statements that could otherwise be abstract and lacking in context. For such a test to truly encompass all circumstances, it must consider the threat from a reasonable person in the victim's position.

In addition, the aggregate nature of communications on interactive websites like Twitter make threats inherently riskier, which should encourage a lower standard. This is important because all people should have the right to free expression online, not just malicious actors.[249] Freedom of expression should "extend[] to those who are too afraid to participate in online activities and debates because of fear of harassment. Their right to express themselves must be protected too."[250]

More specifically, when an actor chooses to publish a subject's home address, she consciously disregards a substantial chance that her words will be perceived as a threat because the publication of the home address moves the harassment from the digital world into the real world, where physical violence can take place.[251] The act approaches a per se true threat because it creates particularity by specifying a location of harm. Of course, an address dox alone, without more, would likely not constitute a true threat. It must be accompanied by a pattern of conduct that includes harassment and particularized threats. Under this solution, the harassment and dox of Brianna Wu would constitute a true threat and be actionable.[252] Accordingly, the recklessness standard will help to make § 875(c) more broadly applicable to doxing cases.

245. *See supra* Part II.A.2.b.

246. *See* Maria A. Brusco, *Read This Note or Else!: Conviction Under 18 U.S.C. § 875(c) for Recklessly Making a Threat*, 84 FORDHAM L. REV. 2845, 2870 (2016). *But see* United States v. Elonis, 841 F.3d 589, 596 (3d Cir. 2016) (declining to specify whether recklessness suffices, but finding that § 875(c) contains both a subjective and objective component); *supra* note 148 and accompanying text.

247. *See* Elonis v. United States, 135 S. Ct. 2001, 2012–13 (2015).

248. *See supra* Part II.A.2.

249. Emma Morris, *Online Harassment: Testing the Limits of Free Speech*, FAM. ONLINE SAFETY INST. (July 26, 2016), https://www.fosi.org/policy-research/online-harassment-testing-limits-free-speech/ [https://perma.cc/WG4E-3XPN].

250. *Id.*

251. CITRON, *supra* note 16, at 102.

252. *See supra* Part II.

B. States Should Criminalize the Malicious Publication of Personal Information

In addition to strengthening the application of existing federal statutes, a comprehensive approach to providing a remedy for malicious doxing would also include new or amended state criminal legislation. State legislation would work in concert with the federal Interstate Stalking and Interstate Communications Statutes because it can be more narrowly tailored. These state laws will fill gaps that cannot be covered by the federal legislation.

It is well established that "'the basic principles of freedom of speech and the press, like the First Amendment's command, do not vary' when a new and different medium for communication appears."[253] Even so, remedies are possible under established exceptions to the First Amendment because "developments in technology influence the appropriate interpretation of constitutional rights."[254] Accordingly, the First Amendment "need not be intentionally blind to the way the Internet has changed the way we interact with one another."[255] New or amended legislation does not need to be restricted to a course of conduct because, as argued in Part III.A, doxes of a person's home address come close to approximating a true threat on their own and thus can be regulated.[256]

State criminalization of doxing is also a more practical solution because subjects call 911 and hope for immediate police intervention when they are threatened. Police, however, have no clear guidelines on how to respond to cybersecurity issues and thus fail to help doxing subjects. Having succinct state laws will enable officers to meet the needs of doxed citizens the moment harassment is reported.

State criminal laws also provide maximum flexibility without burdening doxing subjects. They are preferable over a common law remedy because criminal laws remove the procedural and practical bars to relief.[257] Criminal statutes serve as a "route to deterrence" that does not "put all the burden on victims."[258]

States can look to proposed federal legislation for guidance on how to best craft a criminal doxing statute.[259] At the federal level, other comparable solutions include swatting hoaxes legislation, the Clark bill,[260] and the Speier revenge porn bill.[261] These three legislative solutions

253. Brown v. Entm't Merchs. Ass'n, 564 U.S. 786, 790 (2011) (quoting Joseph Burstyn, Inc. v. Wilson, 343 U.S. 495, 503 (1952)).

254. Leong & Morando, *supra* note 34, at 131.

255. *Id.*

256. *See* discussion *supra* Part III.A.

257. *See supra* Part II.B.2.

258. Emily Bazelon, *Why Do We Tolerate Revenge Porn?*, SLATE (Sept. 25, 2013, 6:21 PM), http://www.slate.com/articles/double_x/doublex/2013/09/revenge_porn_legislation_a_new_bill_in_california_doesn_t_go_far_enough.html [https://perma.cc/5UAS-T6ZP].

259. *See supra* Part II.A.4.

260. *See* discussion *supra* Part II.A.4.

261. *See* Franks, *supra* note 10; *see also Rep. Speier Plans to Reintroduce Revenge Porn Bill in 2017*, IAPP (Oct. 3, 2016), https://iapp.org/news/a/rep-speier-plans-to-reintroduce-revenge-porn-bill-in-2017/ [https://perma.cc/LF6P-LGP7].

provide direction to law enforcement to increase funding and training relating to lesser-known types of online harassment. These solutions are excellent models for how states should attempt to legislate against home address doxes.

Trained, knowledgeable officers can help to overcome threats and make doxing subjects feel safe. To assist states with the enforcement of malicious doxing statutes, Congress should support Representative Clark's law enforcement training bill, providing resources to state and local police departments and prosecutors' offices to ensure that states have the funding they need to enforce newly created or amended laws.[262]

CONCLUSION

The malicious publication of personal information is an online harassment tool that causes unique and serious real-world harms. While the law currently provides effective remedies for subjects who are doxed for political purposes, current federal and state approaches do not provide a consistent, effective legal remedy for purely malicious doxing. Lower federal courts should adopt a recklessness standard for interpreting the interstate communications statute to facilitate enforcement of malicious doxing cases. In addition, states should create criminal laws that offer maximum flexibility and train officers to assist and protect doxing subjects. The increasing use and newsworthiness of malicious doxing as a tool to harass and silence indicates that the time has come to ensure protections are in place so that people can use the Internet without fear of physical violence.

262. *See* discussion *supra* Part II.B.1.