HOW TO CLOSE PANDORA'S DOX: A CASE FOR THE FEDERAL REGULATION OF DOXING

Hannah Shankman[*]

Abstract

Doxing, or the sharing of one's personally identifiable information on the Internet without consent, saw a boom during the COVID-19 pandemic. It became a way for Internet users to punish people for racist, rude, or anti-masking behavior and to quench a collective thirst for justice. While some continue to view doxing as an exercise in accountability, it is a malleable tool that can suit anyone's aim. White supremacists, neo-Nazis, and the alt-right regularly resort to doxing those with whom they disagree. Beyond the harassment, financial harm, and death threats doxing victims face, it is a tactic that is counter to foundational First Amendment values. An omnipresent threat of doxing has the potential to close the marketplace of ideas and suppress the free flow of thought.

Presently, there is no clear protection for doxing victims. Although more and more states are considering legislation and social media websites are attempting to self-regulate, the present mechanisms remain inadequate. Jurisdictional issues, First Amendment concerns, and Section 230 of the Communications Decency Act present huge barriers to effective regulation. Doxing victims pay the price and are left without clear recourse. For these reasons, this Article argues that the federal government must pass anti-doxing legislation to adequately protect against the tactic. This Article proposes a piece of model legislation that addresses doxing's unique features and First Amendment concerns.

INTRODUCTION

You may remember the video. It was posted May 25, 2020—the first summer of the COVID-19 pandemic and on the same day as the murder of George Floyd.[1] The video began with a white woman who picked up a dog by its collar in what looked to be a park.[2] She walked toward the camera and asked the person recording her to stop.[3] The voice behind the camera responded, "Please don't come close to me."[4] At this point, about twenty seconds into the video, things took a turn. The woman proceeded to let the man know that she was going to call the police.[5] She stated, "I am going to tell them that there is an African American man threatening

---

* J.D. 2022, The George Washington University Law School; B.A. 2017, Binghamton University, State University of New York. I would like to thank Professor Dawn C. Nunziato for her guidance and support, my seminar classmates for their encouragement and feedback, and my mother, Julie Shankman, for everything.

1. Megan Phelps-Roper, *The Real Story of "The Central Park Karen*," COMMON SENSE (Aug. 3, 2021), https://bariweiss.substack.com/p/the-real-story-of-the-central-park?s=r [https://perma.cc/9P78-D3UK]. Megan Phelps Roper was raised in the Westboro Baptist Church, which was founded by her grandfather. The church is known for publicly protesting "vices" such as homosexuality, and the church gained notoriety in the 2000s for protesting at the funerals of American soldiers who died in the War in Afghanistan and the War in Iraq. *See* Snyder v. Phelps, 562 U.S. 443, 448 (2011) ("The [Westboro Baptist Church] frequently communicates its views by picketing, often at military funerals. In the more than 20 years that the members of Westboro Baptist have publicized their message, they have picketed nearly 600 funerals."). Ms. Phelps-Roper left the Westboro Baptist Church in 2012 after she began to disagree with the church's teachings. She cites engaging in open dialogue with others on Twitter as the impetus for her changed views. *See* MEGAN PHELPS-ROPER, UNFOLLOW: A MEMOIR OF LOVING AND LEAVING THE WESTBORO BAPTIST CHURCH *passim* (2019).

2. Tamar Lapin, *Video of White Woman Calling Cops on Black Man in Central Park Draws Outrage*, N.Y. POST (May 25, 2020, 8:36 PM), https://nypost.com/2020/05/25/video-of-white-woman-calling-cops-on-black-man-in-central-park-draws-outrage/ [https://perma.cc/428F-4CX6].

3. *Id.*

4. *Id.*

5. *Id.*

my life."[6] She then called the police and said over the phone that an African American man is recording her and threatening her and her dog.[7]

This minute long video was posted to Twitter and went viral.[8] The caption that accompanied the tweet referred to the woman as a "Karen"[9] and informed viewers that this interaction occurred because the man recording asked the woman to comply with Central Park's rules and place her dog on a leash in the Ramble.[10] Twitter users that reposted, commented, and replied to the video were outraged by the white woman weaponizing the man's race against him to the police and deemed her behavior racist.[11]

To quote one user:

> The way she tried to first evoke fear in him by telling him what she was going to say. She knew that those words were a threat to his life. And then she turned around and did it, with increasing faux urgency. While her dumbass was being filmed. White supremacy is a sickness.[12]

Shortly after the video was posted, the Internet[13] identified the woman

---

6. *Id.*

7. *Id.*

8. The Associated Press, *Video Shows White Woman Calling Police on Black Man in Central Park*, N.Y. TIMES (May 27, 2020), https://www.nytimes.com/video/us/100000007159234/amy-cooper-dog-central-park-police-video.html [https://perma.cc/4VRM-T4HQ]. At the time of this Article, the video had been viewed 45 million times on Twitter alone. *See* Troy Closson, *Amy Cooper Falsely Accused Black Bird-Watcher in 2nd 911 Conversation*, N.Y. TIMES (May 26, 2021), https://www.nytimes.com/2020/10/14/nyregion/amy-cooper-false-report-charge.html [https://perma.cc/5S9V-JDKM].

9. "Karen" is a term used to refer to white women that are seen as entitled or rude. Elle Hunt, *What Does It Mean to Be a 'Karen'? Karens Explain*, GUARDIAN (May 13, 2020), https://www.theguardian.com/lifeandstyle/2020/may/13/karen-meme-what-does-it-mean [https://perma.cc/85NK-BS6B].

10. Lapin, *supra* note 2. The Ramble is one area within Central Park, located in New York City, New York.

11. *See, e.g.*, Dr. Shola Mos-Shogbamimu (@SholaMos1), TWITTER (May 26, 2020, 3:03 AM), https://twitter.com/SholaMos1/status/1265176663194841090 [https://perma.cc/FV9R-F4WP] ("Can't express how angry and horrified I am by this RACIST. I'm so glad your brother is OK. This evil against black people must end. Thank you for making this public. Anyone offended by the use of 'Karen' can go rot! #AmyCooper is Karen personified and a #WhiteSupremacist."). Users were also alarmed by the way the woman was handling the dog. *See Tweet*, TWITTER, https://twitter.com/melodyMcooper/status/1264965252866641920?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1264965252866641920%7Ctwgr%5Eshare_3&ref_url=https%3A%2F%2Fwww.nytimes.com%2F2020%2F05%2F26%2Fnyregion%2Famy-cooper-dog-central-park.html [https://perma.cc/M5VF-8SNH] (last visited May 12, 2023).

12. SUMMER'S RENAISSANCE (@EssBreezyBaby), TWITTER (May 25, 2020, 4:39 PM), https://twitter.com/EssBreezyBaby/status/1265019761462775813.

13. At the time of this Article, it is unclear who was the first person to release Amy Cooper's name on the Internet. This is common with instances of doxing, and this Article will discuss this issue in Section I.B.

in the video as Amy Cooper.[14] Within hours of the video's release, her personal phone number and address were posted as well.[15] She started to receive death threats, hundreds of phone calls, and graphic messages.[16] Later that night, a crowd gathered outside her apartment to show their displeasure, and within two days, Franklin Templeton fired Amy from her position at the investment firm.[17] The result of this interaction in the park? Amy Cooper was doxed.

Doxing[18] is a type of cyber-harassment.[19] It involves the online public release of personal information that can be used to identify or locate an individual, usually without the individual's consent.[20] Additionally, there is an unspoken message behind the release of this information: harass the named individual.[21]

You may be wondering: "Why should I care? Amy is merely being held accountable for her racist actions. This is in the public's interest." After experiencing a summer that dealt with a long-overdue racial reckoning, and years of people's repeated refusal to comply with masking measures during a pandemic, an apathy toward a person being doxed and subsequently fired for racist behavior is reasonable. And you would not be alone in this sentiment: since the summer of 2020, viral videos of individuals saying racist things or yelling at employees over being asked to wear a mask inside have become all too common.[22] Consequently, entire TikTok pages dedicated to identifying the people who transgressed in these videos have sprung up and generated millions of views.[23] It seems society has developed a collective thirst for accountability and justice.

---

14. Daniel Johnson, *'Central Park Karen' Defends Her Actions in First Interview Since Fleeing U.S.*, NAT'L POST (Aug. 5, 2021), https://nationalpost.com/news/central-park-karen-defends-her-actions-in-first-interview-since-fleeing-u-s [https://perma.cc/A96T-GZDJ].

15. *Id.*

16. *Id.*

17. *Id.*; Lisette Voytko, *Amy Cooper Fired After Viral Central Park Video*, FORBES (May 27, 2020, 1:09 PM), https://www.forbes.com/sites/lisettevoytko/2020/05/26/amy-cooper-fired-after-viral-central-park-video/?sh=1377333f5c53 [https://perma.cc/N556-CWWA] ("'We have made the decision to terminate the employee involved.' Franklin Templeton wrote on its official Twitter account, adding, 'We do not tolerate racism of any kind.'").

18. Doxing is also sometimes spelled "doxxing."

19. Hannah C. Mery, *The Dangers of Doxing and Swatting: Why Texas Should Criminalize These Malicious Forms of Cyberharassment*, 52 ST. MARY'S L.J. 905, 911 (2021).

20. Alexander J. Lindvall, *Political Hacktivism: Doxing & the First Amendment*, 53 CREIGHTON L. REV. 1, 2 (2019).

21. *Id.*

22. *See* Richard Tribou, *Florida Man Without Mask Seen Shouting at Costco Fired from Job*, ORLANDO SENTINEL (July 8, 2020, 7:16 AM), https://www.orlandosentinel.com/news/florida/os-ne-florida-man-without-mask-costco-video-fired-from-job-20200708-s2o767gqzbetljip7w5h7tdiqi-story.html [https://perma.cc/P8KX-5QC4].

23. *See* TizzyEnt (@tizzyent), TIKTOK, https://www.tiktok.com/@tizzyent [https://perma.cc/J5VW-LQWR]; Danesh (@thatdaneshguy), TIKTOK, https://www.tiktok.com/@thatdaneshguy?lang=en [https://perma.cc/U529-Q9M8].

Posting people's names, places of employment, addresses, and phone numbers provides a mechanism to quench this thirst.

While doxing is a way to punish people for their perceived crimes,[24] the sentence that results can be lifelong and severe.[25] Doxing has repeatedly led to death threats, harassment, and job loss for those that are doxed.[26] As reporter Zeeshan Aleem points out, job loss is especially harsh in the American social scheme because there is a weak social safety net, and it often results in the additional loss of one's health care.[27] Further, a person who is doxed often becomes "radioactive" on the job market and unhirable down the line.[28] With the doxers playing the judge, jury, and executioner based on minute-long videos, we as a society need to reckon with whether this punishment tactic should be permitted to continue.

This question becomes even more poignant when you consider doxing's malleability. It is a tool that can be used by any group to suit any aims. Indeed, the Amy Coopers of the world are not the only people that are doxed. White supremacists, neo-Nazis, and the alt-right have regularly resorted to doxing people whose views they disagree with.

Damon Young, a black writer, editor, and critic for *The New York Times*, *The Washington Post*, and *GQ*, is one example. He was doxed by white supremacists after he published an article, "Whiteness Is a Pandemic," about the March 2021 Atlanta shooting of six Asian women.[29] Tanya Gersh, a Jewish real estate agent from Whitefish, Montana, is another.[30] She had her phone number published on the *Daily Stormer*, a

---

24. Dylan E. Penza, *The Unstoppable Intrusion: The Unique Effect of Online Harassment and What the United States Can Ascertain from Other Countries' Attempts to Prevent It*, 51 CORNELL INT'L L.J. 297, 304 (2018) ("Many 'doxxers' see this behavior as a form of vigilante justice wherein they reveal the information of people in order to punish them for perceived crimes.").

25. Johnson, *supra* note 14 (Amy Cooper has since left the United States and lives in undisclosed foreign country. She states that she "wishes to move to a non-english speaking country where the story did not run.").

26. *Cancel Culture, Part 2: A Case Study*, N.Y. TIMES (Aug. 11, 2020) [hereinafter *Cancel Culture*], https://www.nytimes.com/2020/08/11/podcasts/the-daily/cancel-culture.html [https://perma.cc/X926-YDV2].

27. *Id.*

28. *Id.*

29. Damon Young, *The Second Best Thing About Getting Doxed by White Supremacists*, WASH. POST (Jan. 31, 2022), https://www.washingtonpost.com/magazine/2022/01/31/damon-young-second-best-thing-about-getting-doxed-by-white-supremacists/ [https://perma.cc/3ATD-V5T4][hereinafter *The Second Best Thing*]; Damon Young, *Whiteness Is a Pandemic*, ROOT (Mar. 17, 2021, 1:00 PM), https://www.theroot.com/whiteness-is-a-pandemic-1846494770 [https://perma.cc/96JZ-B57L] [hereinafter *Whiteness*].

30. Elizabeth Williamson, *How a Small Town Silenced a Neo-Nazi Hate Campaign*, N.Y. TIMES (Nov. 8, 2021), https://www.nytimes.com/2021/09/05/us/politics/nazi-whitefish-charlottesville.html [https://perma.cc/7T7E-37XR].

popular neo-Nazi website, after she was involved with a real estate dispute with the mother of Richard B. Spencer, a white nationalist alt-right leader.[31] Female video game developers Zoe Quinn and Brianna Wu, and feminist media critic Anita Sarkeesian, are other examples.[32] They were doxed and suffered years-long misogynistic online harassment, including death threats and threats of rape, because they advocated for more inclusivity in video games in the cultural phenomenon now known as "GamerGate."[33] The list of those doxed by white supremacists goes on and on.

Given these realities, this Article argues that doxing poses a substantive harm and should be regulated by the federal government. Not only can doxing lead to intimidation, harassment, financial harms, and leave those who are doxed fearing for their life, it is a tactic that doxers can use to entirely stifle speech. Eleven states have recognized this danger and passed doxing prohibitions or strengthened existing laws to include this tactic, and three more states are currently considering doxing legislation.[34] However, state regulation is inadequate. These Internet interactions rarely happen entirely within state lines, and perpetrators are likely beyond the reach of a state court's jurisdiction. This Article argues that the federal government needs to pass anti-doxing legislation to adequately protect against the tactic.

This Article proceeds in five parts. Part I provides a general definition of doxing and discusses specific aspects of the tactic that make it unique. This part includes a discussion of First Amendment issues as they pertain to doxing's regulation. Part II outlines the ways doxing could be regulated, including self-regulation by social media websites, state by state regulation, and federal legislation. Part III then explains why federal legislation provides the best chance to combat doxing. Next, Part IV provides a model piece of federal legislation, and explains why the proposed legislation would likely survive a First Amendment challenge. Finally, Part V concludes.

---

31. *Id.*; *Richard Bertrand Spencer*, S. POVERTY L. CTR., https://www.splcenter.org/fighting-hate/extremist-files/individual/richard-bertrand-spencer-0 [https://perma.cc/SJ5B-69QG] (last visited Mar. 18, 2022).

32. Caitlin Dewey, *The Only Guide to Gamergate You Will Ever Need to Read*, WASH. POST (Oct. 14, 2014), https://www.washingtonpost.com/news/the-intersect/wp/2014/10/14/the-only-guide-to-gamergate-you-will-ever-need-to-read/ [https://perma.cc/4FGX-UWLH].

33. *Id.*

34. Emma Betuel, *Should Doxing Be Illegal?*, MARKUP (Aug. 17, 2021, 8:00 AM), https://themarkup.org/ask-the-markup/2021/08/17/should-doxxing-be-illegal [https://perma.cc/6GQ7-UH2H].

I. DEFINING DOXING AND ITS UNIQUE FEATURES

Though doxing entered mainstream channels over ten years ago[35] and has seen a boom in the last five years,[36] most attribute the origins of the tactic to hackers in the 1990s.[37] Hackers would post fellow users' personal information as a means of retaliation during an argument.[38] The term "dox" comes from the abbreviated form of documents: "docs."[39] It is a nod to the fact that Internet users could use documents to reveal a formerly anonymous person's identity.[40] Users would then "drop" the documents to reveal one's identity.[41] Over time, this methodology took on the term "doxing."[42]

A. *Doxing: Toward a General Definition*

Today, legislators and academics define the term as sharing someone's "personal information" or "personally identifiable information" on the Internet.[43] These definitions also recognize a certain intent on behalf of the doxer. To constitute doxing, the doxer must intend a level of harassment toward the target by releasing their information.[44] The doxer can either intend to cause this harassment themselves or simply serve as a facilitator and leave the harassment to those that view the posted information.[45]

Definitions of doxing tend to use the broad term "personally identifiable information" because each instance does not necessarily involve the same release of information.[46] While, at a minimum, doxing involves the online publication of a target's full name, the additional information that

35. Megan Garber, *Doxing: An Etymology*, ATLANTIC (Mar. 6, 2014), https://www.theatlantic.com/technology/archive/2014/03/doxing-an-etymology/284283/ [https://perma.cc/T2F5-VZPM].

36. Nellie Bowles, *How Doxing Became a Mainstream Tool in the Culture Wars*, N.Y. TIMES (Aug. 30, 2017), https://www.nytimes.com/2017/08/30/technology/doxxing-protests.html [https://perma.cc/L9RE-E9RS].

37. Garber, *supra* note 35.

38. *Id.*

39. *Id.*

40. *Id.*

41. Michelle Park, *The Doxing Guide: What It Is, Statistics, Legality, and Prevention*, GARBO (Aug. 16, 2021), https://www.garbo.io/blog/doxing [https://perma.cc/K8KY-FJNH].

42. Garber, *supra* note 35.

43. *See* Lisa Bei Li, *Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting*, 70 FED. COMMC'NS L.J. 317, 326 (2018); Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. (2016).

44. Lindvall, *supra* note 20, at 8; Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. (2016).

45. Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. (2016).

46. Svana Calabro, *From the Message Board to the Front Door: Addressing the Offline Consequences of Race- and Gender-Based Doxxing and Swatting*, 51 SUFFOLK U. L. REV. 55, 67 (2018).

is released beyond one's name varies. It can include phone numbers, work and home addresses, emails, social security numbers, employer contact information, or some combination of this information.[47] Put simply, there is not one uniform way doxers dox; therefore, the definition is intentionally broad to capture each variation.

Legislators and academics also consider doxing a type of "cyber-harassment."[48] It is typically grouped with cyber-stalking, cyber-bullying, and swatting because there is significant overlap between these acts' definitions.[49] For example, cyber-stalking is where a perpetrator uses social media, Internet databases, and other online resources to repeatedly intimidate, terrorize, threaten, or cause fear in another person.[50] Often, the cyber-stalker is personally acquainted with their victim, and in many cases, the perpetrator and victim had a romantic relationship.[51]

Similarly, cyber-bullying is defined as "the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature,"[52] and "the electronic posting of mean-spirited messages about a person (such as a student) often done anonymously."[53] Swatting is another variation of cyber-harassment.[54] It is where a person falsely reports an emergency at a victim's home—such as a hostage situation or active shooter—to bait the police into sending a Special Weapons and Tactics (SWAT) team to the victim's home.[55] The idea is the SWAT team will enter the target's home with guns drawn, and at a minimum, terrify the unsuspecting victim.[56]

Doxing is similar to these other forms of cyber-harassment because they all have goals of instilling fear, causing intimation, and harassing the target. However, as the tactic currently stands, doxing contains a few

---

47. Patricia R. Recupero, *New Technologies, New Problems, New Laws*, 44 J. AM. ACAD. PSYCHIATRY & L. 322, 325 (2016); Lindvall, *supra* note 20; Dylan E. Penza, *The Unstoppable Intrusion: The Unique Effect of Online Harassment and What the United States Can Ascertain from Other Countries' Attempts to Prevent It*, 51 CORNELL INT'L L.J. 297, 303–04 (2018).

48. Penza, *supra* note 47; Calabro, *supra* note 46; *Clark Bill Criminalizes Malicious Publication of Private Information*, KATHERINE CLARK 5TH DIST. OF MASS. (Dec. 8, 2016), https://katherineclark.house.gov/press-releases?ID=845879BE-5C95-4115-A5ED-A4BD79CA611B [https://perma.cc/Y3E3-PFEN].

49. Penza, *supra* note 47; Ioana Vasiu & Lucian Vasiu, *Light My Fire: A Roentgenogram of Cyberstalking Cases*, 40 AM. J. TRIAL ADVOC. 41, 43 (2016).

50. Sameer Hinduja, *Cyberstalking*, CYBERBULLYING RSCH. CTR., https://cyberbullying.org/cyberstalking [https://perma.cc/4BRP-2ATU] (last visited May 13, 2023).

51. Vasiu & Vasiu, *supra* note 49.

52. *Cyberbullying*, OXFORD DICTIONARY (3d ed. 2010).

53. *Cyberbullying*, MERRIAM WEBSTER, https://www.merriam-webster.com/dictionary/cyberbullying [https://perma.cc/267B-TJKA] (last visited May 13, 2023).

54. Penza, *supra* note 47, at 304.

55. *Id.* at 304 n.50; Calabro, *supra* note 46, at 60.

56. *See* Calabro, *supra* note 46, at 56 (describing the 2016 swatting of Congresswoman Katherine Clark).

unique qualities that distinguishes it from other forms of cyber-harassment. These distinctive features are important to keep in mind when thinking about how to appropriately address doxing.

B. *Doxing's Unique Features*

The main unique features of doxing are the: (1) semi-public nature of the information released by doxers; (2) doxing's accountability feature; (3) the involvement of multiple actors; and (4) free speech concerns. Notably, these are also the main themes that underscore many of the arguments against doxing regulation.[57] This section will address each in turn.

1. The Information Is Already Public

First, the information that is released in a doxing episode has a varying degree of "publicness."[58] Home addresses can be found with a quick search online through "whitepages.com" or "peoplefinder.com,"[59] and doxers are often using public information that does not require a hack to access.[60] Rather, doxers are simply gathering information from sites like LinkedIn, Facebook, or Google.[61] For this reason, some argue that legislators should not regulate doxing, as perpetrators only use a victim's public information.[62] As the Supreme Court noted in *Cox Broadcasting Corp. v. Cohn*, "interests in privacy fade when the information involved already appears on the public record."[63]

These are valid concerns; yet, focusing on the nature of information ignores a few important points. For one, there is a difference between personally identifiable information existing on the Internet as various independent data points, and a post curated to host all of one's personally identifiable information in one place.[64] The latter presents a level of accessibility, to the millions of people on the Internet, to whom this information was not previously available. And this is all done without the con-

57. I would like to thank my peers for raising many of these concerns while I was writing this Article.

58. Julia M. MacAllister, *The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information*, 85 FORDHAM L. REV. 2451, 2456 (2017).

59. *See* Nicole Levine, *How to Find a Current Address for Someone*, WIKIHOW (Mar. 15, 2022), https://www.wikihow.com/Find-a-Current-Address-for-Someone [https://perma.cc/W6ZP-U48M] (describing what online websites to use to find a person's address).

60. MacAllister, *supra* note 58.

61. Zaraki Kenpachi, *How to Dox Someone on TikTok*, SELFOY (Jan. 5, 2022), https://selfoy.com/how-to-dox-someone-on-tiktok-know-more-about-it/ [https://perma.cc/CS9B-V4GG].

62. MacAllister, *supra* note 58, at 2458.

63. Cox Broad. Corp. v. Cohn, 420 U.S. 469, 494–95 (1975).

64. MacAllister, *supra* note 58, at 2458.

sent of the person to whom the information belongs. A doxing post fundamentally concentrates and alters the nature of the information. It turns it into a weapon that can be used by anyone who views it.

Furthermore, not all the information doxers release is publicly accessible.[65] For example, personal cell phone numbers are not generally considered part of the public record, and social security numbers are clearly private.[66] To say that doxing strictly involves public information is an overstatement.

Lastly, prohibitions against doxing are not solely rooted in the "interest in privacy" or in the "zone of privacy that surrounds every individual" that is discussed in *Cox Broadcasting*.[67] Rather, proposed doxing regulations are also focused on the malicious and threatening intent of the doxer in posting the target's information.[68] While doxing arguably invades the privacy of the victim, doxers are also using this information—both public and private—to *intentionally* cause serious financial and reputational harms, emotional distress, death threats, and sustained harassment and intimidation.[69] This should help distinguish doxing from other privacy cases where the Supreme Court has said protections were limited because of the public nature of information.

2. A Good Faith Dox?

Next, some argue doxing is not qualitatively the same as other forms of cyber-harassment. Unlike cyber-stalking or cyber-bullying, where malignant aims are foundational to the perpetrator's goals, a doxer may not consider themselves as holding a malicious intent.[70] Doxers could view themselves as seeking justice and holding those that transgress accountable.[71] Popular TikTok users hold this view and portray themselves as engaging in a type of "good faith" awareness campaign.[72]

---

65. Park, *supra* note 41.

66. Frayda Bluestein, *Are Cell Phone Bills Public Records*, COATES' CANNONS NC LOC. GOV'T L. (Oct. 5, 2011), https://canons.sog.unc.edu/2011/10/are-cell-phone-bills-public-records/ [https://perma.cc/M3CB-H6RK].

67. *Cox Broad. Corp.*, 420 U.S. at 487.

68. Lindvall, *supra* note 20, at 5.

69. Penza, *supra* note 47, at 305–08; *Cancel Culture*, *supra* note 26.

70. Penza, *supra* note 47, at 304.

71. *Id.*

72. Ryan Broderick, *TikTok Drama Channels Are Turning into Online Intelligence Agents*, VERGE (Dec. 6, 2021, 8:30 AM), https://www.theverge.com/22809838/tiktok-drama-channels-osint-antivaxx-doxxing-creators [https://perma.cc/MYC5-9VBD] ("[Michael] Mc told *The Verge* he's trying to bring some accountability back to how people behave on the internet."); Penza, *supra* note 47, at 304 n.45 ("Perhaps the most well known recent case of doxxing as vigilante justice took place after the white supremacist rally in Charlottesville last August, where in internet users, most notably Twitter user @YesYoureRacist tried to release the identities of those who attended the rally.").

This nuance is particularly relevant when a person is doxed after a video of them acting in a racist manner goes viral, and Internet users subsequently contact the person's place of employment. Returning to the case of Amy Cooper highlights this point. Many would argue that Franklin Templeton *should* have the ability to terminate a racist employee, and the doxers are simply bringing this information to the employer's attention. One may argue that doxing should be permitted because it provides this ability to bring awareness to transgressions.

These concerns are easily addressed by a well-drafted statute. A doxing statute could limit the prohibition to the *malicious* publication of personally identifiable information.[73] A statute could then define malicious publication as the posting of such information with the intent to "threaten, intimidate, harass, stalk."[74] Adding this mal-intent requirement would help distinguish between doxing that is premised on causing harm and socially beneficial forms of online identification.[75] The intent precondition creates a needed balance: barring doxing rooted in harassment while permitting good faith awareness campaigns.

Of course, there may be cases where it is questionable whether the doxers are genuinely engaged in a "good faith" awareness campaign. In such instances, the court would have to judge the behavior on a case-by-case basis and look at the surrounding context to determine if the necessary mal-intent was present. Proving the necessary intent is common feature of the American legal system, and such an inquiry for doxing would be no different.

3. Multiple Actors and Different Roles

Doxing rarely involves the action of a singular perpetrator.[76] A doxing campaign usually comprises action on behalf of multiple actors collectively partaking in different roles: some releasing the personally identifiable information, some contacting the victim, and others engaging in both genres of action.[77] This creates the question of who involved in the tactic should be held liable and what behaviors should trigger liability.

Again, this difficulty could be solved by the drafting of the doxing statute. The statute could attach liability for the person that initially posts personally identifiable information as well as for people who facilitate,

---

73. MacAllister, *supra* note 58, at 2457–59.

74. Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. (2016).

75. *Doxing Should Be Illegal. Reporting Extremists Should Not*, AM. DEFAMATION LEAGUE (Jan. 15, 2021), https://www.adl.org/blog/doxing-should-be-illegal-reporting-extremists-should-not [https://perma.cc/E9CM-ANAX].

76. MacAllister, *supra* note 58.

77. MacAllister, *supra* note 58, at 2474 (stating that actors can work together in a "cybermob," with "one poster starting the abuse and others piling on").

assist, or promote the posting of such information.[78] This additional liability for the facilitation of doxing would help capture the "conspiratorial" doxers—the individuals who are not necessarily the initial poster. There may still be questions surrounding the identity of the defendant, but these are tactical questions that plaintiffs and prosecutors must regularly decide based on available evidence. Nevertheless, the suggested statutory language would provide victims the opportunity for recourse in the common scenario when there is not one sole doxer.[79]

4. First Amendment Free Speech Concerns

Lastly, doxing implicates concerns rooted in the freedom of expression. The first free speech concern is that the public can use doxing, or the threat of doxing, to stifle speech. Individuals could dox those with whose viewpoints they disagree instead of responding with alternative narratives or counter speech. Gamergate and Damon Young's doxing are examples of this.[80] The women of Gamergate were doxed after criticizing the video game culture and advocating for greater inclusion for women in the video game field.[81] Writer Damon Young was doxed after critically analyzing how whiteness, and white supremacy, led to the March 16, 2021, murders of six Asian American women in Atlanta.[82]

If people must be concerned about the release of their personally identifiable information and the inevitable harassment that follows when they share opinions, they may become reluctant to share their points of view. This is concerning because an "open marketplace" of ideas is central to the First Amendment and to democracy.[83] An omnipresent threat of doxing has the potential to close the marketplace and suppress the free flow of thought. This is counter to foundational First Amendment values and provides another reason why doxing should be regulated.

The second concern centers on the doxing post itself: doxers argue their posts are protected free speech.[84] While doxing is speech,[85] and the

78. Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. (2016); L.B. 227, 107th Leg., 1st Sess. (Neb. 2021).

79. Betuel, *supra* note 34.

80. Dewey, *supra* note 32; *The Second Best Thing*, *supra* note 29.

81. Dewey, *supra* note 32.

82. *The Second Best Thing*, *supra* note 29.

83. Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting); Red Lion Broad. Co. v. FCC, 395 U.S. 367, 390 (1969).

84. *See* Gersh v. Anglin, 353 F. Supp. 3d 958, 963 (D. Mont. 2018) ("Anglin contends that his motion to dismiss should be granted because the speech giving rise to Gersh's claim enjoys First Amendment protection. He argues that: (1) the speech does not fall within an unprotected category; and (2) the speech involved both a matter of public concern.").

85. *See* Brush & Nib Studio, LC v. City of Phoenix, 448 P.3d 890, 905 (Ariz. 2019) ("Pure speech includes written and spoken words, as well as other media such as paintings, music, and film 'that predominantly serve to express thoughts, emotions, or ideas.'").

First Amendment prevents Congress and the states from enacting any law that abridges the freedom of speech,[86] the analysis of whether First Amendment protections apply in these cases is not necessarily that cut and dry. For one, protections do not apply when the government restricts "unprotected" speech,[87] such as obscenity,[88] true threats,[89] fighting words,[90] or incitement.[91] In instances of these categories of speech, the government is free to restrict its use. The Court has also emphasized that the level of First Amendment protection depends on the public significance of the speech.[92] For speech on matters of private concern, "First Amendment protections are often less rigorous."[93] Comparatively, matters of public concern are at the heart of the First Amendment and strongly protected.[94]

While the First Amendment also prevents the government from regulating speech based on its content or the viewpoints expressed,[95] courts have upheld statutes that regulate speech based on content.[96] To be clear, statutes containing content-based restrictions are considered especially pernicious, presumptively invalid,[97] and must survive the often-fatal inquiry of "strict scrutiny,"[98] but it has been done.[99] To do so, the government must show the statute serves a compelling interest, and that the government has regulated the speech by the least restrictive means.[100]

In evaluating the constitutionality of a doxing regulation, a court would first need to determine whether doxing constitutes unprotected or protected speech.[101] Some academics have argued that doxing could fall into the true threat exception and constitute unprotected speech.[102] After

86. U.S. CONST. amend. I.
87. Nev. Comm'n on Ethics v. Carrigan, 564 U.S. 117, 121 (2011).
88. Miller v. California, 413 U.S. 15, 22 (1973).
89. Watts v. United States, 394 U.S. 705, 708 (1969).
90. Chaplinsky v. New Hampshire, 315 U.S. 568, 571–72 (1942).
91. Brandenburg v. Ohio, 395 U.S. 444, 449 (1969).
92. Snyder v. Phelps, 562 U.S. 443, 451–52 (2011).
93. *Id.* at 452.
94. *Id.* at 451–52.
95. City of Los Angeles v. Alameda Books, Inc., 353 U.S. 425, 434 (2002).
96. *See* Burson v. Freeman, 504 U.S. 191, 193, 211 (1992) (holding that a Tennessee statute "prohibit[ing] the solicitation of votes and the display or distribution of campaign materials within 100 feet of the entrance to a polling place" survived strict scrutiny and was constitutional under the First Amendment).
97. *Alameda Books, Inc.*, 353 U.S. at 434.
98. *Id.* at 434.
99. *See, e.g.*, *supra* note 96.
100. *Id.* at 455.
101. Brown v. Ent. Merchs. Ass'n, 564 U.S. 786, 790, 799 (2011).
102. *See* MacAllister, *supra* note 58, at 2465 ("The exception most relevant to this Note's effort to find a remedy for doxing is the 'true threat' exception."); Lindvall, *supra* note 20, at 5 ("These [doxing] statutes' mens rea requirements should allow them to fall into the First Amendment's true-threats exception.").

all—like a threat—doxing and the harassment that follows can cause a victim to fear impending violence, bodily harm, or death. It is unclear whether this argument would be convincing for a court. The Supreme Court has limited true threats to instances where "the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals."[103] Though true threats may be implied,[104] a "threat" is premised on actions yet to come. A threat articulates acts the speaker has "intent to commit."[105] With doxing, part of the harm has already occurred when the doxer posts the personally identifiable information. For this reason, and the limited scope of the true threats doctrine, it is far from certain a court would consider doxing a true threat.

Nonetheless, even if a court determined doxing was protected speech, the inquiry would not end. Speech protected by the First Amendment can still be constitutionally regulated if the regulation passes intermediate or strict scrutiny.[106] Strict scrutiny applies when the speech is content based, and intermediate scrutiny applies when the speech is content neutral.[107] A court is likely to consider an anti-doxing statute to be content based. As the Supreme Court has noted, "[g]overnment regulation of speech is content based if a law applies to particular speech because of the topic discussed or the idea or message expressed."[108] An anti-doxing statute is content based because it will regulate based on the type of information the perpetrator releases: personally identifiable information.

Consequently, an anti-doxing statute would likely need to pass strict scrutiny for a court to uphold the regulation. While often fatal, an anti-doxing statute may be able to survive strict scrutiny if the statute closely connects doxing to matters of private concern. Speech on purely private matters "does not carry as much weight in the strict scrutiny analysis as speech concerning matters of public concern."[109] Courts have been willing to find compelling government interests and uphold content-based statutes in instances of non-consensual pornography (NCP).[110] A doxing

103. Virginia v. Black, 538 U.S. 343, 359 (2003).

104. Nat'l Coal. on Black Civic Participation v. Wohl, 498 F. Supp. 3d 457, 479 (S.D.N.Y. 2020).

105. *Black*, 538 U.S. at 359.

106. Holder v. Humanitarian L. Project, 561 U.S. 1, 27–28 (2010).

107. Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989); Reed v. Town of Gilbert, 576 U.S. 155, 163 (2015).

108. *Reed*, 576 U.S. at 163.

109. State v. VanBuren, 214 A.3d 791, 808 (Vt. 2019).

110. *See id.* at 794 (upholding the constitutionality of a Vermont statute banning disclosure of NCP); State v. Casillas, 952 N.W.2d 629, 634 (Minn. 2020) (finding that a Minnesota statute criminalizing the non-consensual dissemination of private sexual images did not violate the First Amendment because it survived strict scrutiny); State v. Katz, 179 N.E.3d 431, 439 (Ind. 2022)

statute modeled on these NCP statutes, too, could be upheld. Therefore, arguing doxing constitutes "free speech" does not end the inquiry surrounding regulation—an anti-doxing statute could be carefully crafted to pass strict scrutiny. This Article will provide one such statute but will first discuss why doxing-specific legislation is the best way to regulate the tactic.

II. WAYS TO COMBAT DOXING

There are a few possible ways to address doxing. First, social media sites could regulate the practice on their own. Second, states could either let traditional tort law handle the practice, or they could decide to pass legislation and attach criminal or civil liability to doxing. Finally, Congress could enact federal legislation to proscribe doxing. As described below, federal criminal legislation is the optimal option because this would avoid the jurisdictional issues involved with state statutes, protect citizens in every state against the tactic, and provide the best chance for an exception to Section 230 immunity.

A. *Regulation by Social Media Companies*

Self-regulation by social media sites is a logical place to begin the inquiry of how to address doxing. Doxing tends to occur on these websites, and many social media websites already have policies in place concerning the practice.[111] For example, Twitter prohibits posting a person's home address or physical location information; identity documents; contact information, "including non-public personal phone numbers or email addresses"; financial account information; and biometric data without permission from whom the information belongs.[112] Tweets containing such information may be removed, and the perpetrator's Twitter account may be suspended.[113]

Similarly, Meta, the media conglomerate that is the parent company to Instagram and Facebook, prohibits doxing.[114] Specifically, Meta pro-

(holding that a Indiana statute criminalizing the non-consensual distribution of an intimate image was constitutional).

111. *See, e.g.*, *Private Information and Media Policy*, TWITTER HELP CTR., https://help.twitter.com/en/rules-and-policies/personal-information [https://perma.cc/W8L2-72H3] (last visited May 13, 2023) ("Sharing someone's private information online without their permission, sometimes called doxxing, is a breach of their privacy and of the Twitter Rules.").

112. *Id.*

113. *Id.*

114. *Privacy Violations*, META TRANSPARENCY CTR., https://transparency.fb.com/policies/community-standards/privacy-violations-image-privacy-rights/ [https://perma.cc/P5K3-6CZJ] (last visited Apr. 29, 2023) (stating that Facebook removes "content that shares, offers or solicits

hibits sharing or soliciting government-issued numbers related to personal identity, such as social security or passport numbers, private contact information like phone numbers, physical addresses, email addresses, and financial information.[115]

Finally, TikTok does not permit doxing on its platform.[116] TikTok's community guidelines define doxing as the act of "collecting and publishing personal data or personally identifiable information (PII) for malicious purposes."[117] The site goes on to define PII as including "residential address, private email address, private phone number, bank statement, social security number, or passport number."[118]

Though the most popular social media sites have policies against doxing, users on the platform are at the mercy of the social media site. This means users are subject to the site's determination of what constitutes doxing and what does not, as well as the site's removal decision. To have any social media post taken down, a user must often first "report" a post.[119] The social media site then evaluates the post and decides whether the content violates its "community guidelines" or "rules" before it takes

---

personally identifiable information or other private information that could lead to physical or financial harm, including financial, residential, and medical information, as well as private information obtained from illegal sources"); *Exposed Private Information*, INSTAGRAM HELP CTR., https://www.facebook.com/help/instagram/122717417885747 [https://perma.cc/5VY2-DGCB] (last visited Apr. 29, 2023) ("Posting private and confidential information is a violation of our Terms of Use. Private and confidential information includes, but isn't limited to, credit card information, social security or alternate national identity numbers, private address or location information, non-public phone numbers and non-public email addresses.").

115. *Privacy Violations*, *supra* note 114. Meta recently strengthened its doxing policy after its oversight board—the governing body in charge of Facebook's and Instagram's content decisions—recommended it do so. The updated policy against doxing no longer permits users to share private residential information, even when the information was publicly available online. *See* Meera Navlakha, *Meta Won't Let People Share Private Home Information Anymore*, MASHABLE (Apr. 11, 2022), https://mashable.com/article/meta-private-residential-home-information-doxxing#:~:text=The%20policy%20change%20will%20further%20protect%20victims%20of%20doxxing.&text=Meta%20will%20no%20longer%20allow,information%20is%20publicly%20available%20online [https://perma.cc/N3EL-L46Q].

116. *Community Guidelines*, TIKTOK, https://www.tiktok.com/community-guidelines?lang=en [https://perma.cc/9NGG-HX9E] (last updated Mar. 2023).

117. *Id.*

118. *Id.*

119. Due to the vast volume of content posted on social media websites, most sites have their own automated content evaluation in addition to flagging by users. *See* Rep. of the Special Rapporteur on the Promotion & Prot. of the Right to Freedom of Op. & Expression, U.N. Doc. A/HRC/38/35, at 12 (2018) [hereinafter Rep. of the Special Rapporteur]. This means sites are regularly evaluating content without any prompting. *See id.* However, the algorithms used to automatically moderate content have raised concerns of "overblocking," and given the volume of content generated on a social media site, these algorithms are unable to capture every violation of the site's guidelines. *See id.*; *see Privacy Violations*, *supra* note 114.

it down.[120] If a user disagrees with the site's determination, the user has limited options. This is especially true for those that disagree with the site's decision to keep content on the site. A user that had their content taken down may appeal the site's enforcement decision,[121] but a user that reported a post, to no avail, has no clear recourse.[122] A user could continue to report content they want taken down, or hope that the site's automated content evaluation algorithm independently removes the post, but again, the user must rely on the social media site to take appropriate action. Put simply, there is no way to *force* a social media website to remove content or to comply with its own internal community guidelines. Rather, users are at the mercy of the site's own regulation and enforcement decisions.

Section 230 of the Communications Decency Act (CDA) further crystalizes this reality because it precludes external regulation of a site's content. Enacted in 1996, Section 230(c)(1) of the CDA provides "[n]o 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."[123] Section 230(c)(1) distinguishes between the users on computer services who create content and the computer service provider that gives people access to that content.[124] Courts have deemed Google, Yahoo!, Facebook, and Craigslist all to be "interactive computer service" providers.[125]

Courts have interpreted Section 230(c)(1) to bar "lawsuits seeking to hold a service provider liable for its exercises of a publisher's traditional

120. *See Private Information and Media Policy*, *supra* note 111 (explaining that, when reviewing reports under its policy, Twitter "consider[s] a number of things," such as what type of information is being shared, who is sharing the information, whether the information is available elsewhere online, and why is the information being shared).

121. *See Our Range of Enforcement Options*, TWITTER HELP CTR., https://help.twitter.com/en/rules-and-policies/enforcement-options [https://perma.cc/52HM-6W7D] (last visited Apr. 30, 2022) (stating that when a tweet is removed, the user who generated the tweet can appeal the decision if they believe there was an error); *Account Safety*, TIKTOK, https://support.tiktok.com/en/safety-hc/account-and-user-safety/account-safety [https://perma.cc/UZY3-2PZC] (last visited May 18, 2023) (noting a TikTok user whose account is banned or video is removed can submit an appeal if the user believes it was incorrectly removed or banned); *Appealed Content*, META (Jan. 19, 2022), https://transparency.fb.com/policies/improving/appealed-content-metric/ [https://perma.cc/7GTT-35W5] ("To appeal a decision on Facebook, people select the option to 'Request Review' after we notify them that their content has been removed or covered with a warning. When a review is requested, Meta reviews the post again and determines whether or not it follows our Community Standards.").

122. *See* Rep. of the Special Rapporteur, *supra* note 119 (emphasizing that appeals are permitted when content is removed).

123. 47 U.S.C. § 230(c)(1) (2018).

124. VALERIE C. BRANNON & ERIC N. HOLMES, CONG. RSCH. SERV., R46751, SECTION 230: AN OVERVIEW 3 (2021).

125. *Id.*

editorial functions—such as deciding whether to publish, withdraw, postpone or alter content."[126] This means that social media sites enjoy a broad immunity against civil suits for the content posted on their website because they simply publish the content and do not generate the content.[127] Section 230 has been effectively used to shield websites against claims that the user generated content on the site constituted "defamation, privacy invasions, intentional infliction of emotional distress, and civil rights violations."[128] As some scholars have noted, the immunity associated with Section 230 provides little incentive for sites to self-regulate the content on their sites.[129]

In terms of doxing, those who feel they have been doxed on social media must first hope that the social media site considers the post to be violative of community guidelines. If the site does not view the post as violating community guidelines, the post will remain accessible for other users to see. Then, even in instances where a user clearly violated a website's guidelines, Section 230 would preclude a user from suing a social media site if it does not effectively enforce their doxing policy.[130] Section 230 also completely removes social media from facing civil liability.[131] Consequently, those that are doxed on a social media site are unable to sue the site for facilitating the doxing.[132]

Barnes v. Yahoo!, Inc. is a perfect example of how these social media realities hurt victims. In *Barnes*, the victim's ex-boyfriend created a fake Yahoo! public profile of her and posted nude pictures of her taken without her consent.[133] The ex-boyfriend also posted her personal phone number, work phone number, work address, and personal address on the profile.[134] The ex-boyfriend went on to use the fake profile to try and solicit sex from others on the site's chatroom.[135] After receiving numerous phone calls, emails, and personal visits from unknown men, the victim utilized Yahoo!'s own procedures to try and have the site take the fake profile down.[136] These attempts failed, and the victim then sued Yahoo! for negligently failing to take down the unauthorized profile.[137] The court held that Section 230 shielded Yahoo! from liability on this basis.[138]

126. Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).
127. BRANNON & HOLMES, *supra* note 124.
128. MacAllister, *supra* note 58, at 2468.
129. *Id.*
130. *Id.* at 2467.
131. *Id.*
132. *Id.* at 2468.
133. Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1098 (9th Cir. 2009).
134. *Id.*
135. *Id.*
136. *Id.* at 1098–99.
137. *Id.* at 1099.
138. *Id.* at 1105.

While many advocate for the CDA's overhaul, political support for such change remains to be seen.[139] While an amended CDA would help doxing victims, an amended Section 230 would not provide victims a direct way to pursue the doxer. Instead, an amendment would remove the site's immunity and permit a victim to sue the site if they were doxed. Victims would still have to rely on the policies and guidelines enacted by the social media sites. Comparatively, legislation would provide a direct and much-needed path for victims to challenge the tactic.

B. *State-by-State Regulation*

State-by-state regulation is another route to address doxing. This could be accomplished by victims using common law tort claims or specific anti-doxing legislation. Most states have not yet legislated against the practice.[140] In such instances, doxing victims would have to try and pursue a tort law claim against the doxer.[141] The victim could file a defamation, harassment, or intentional infliction of emotional distress (IIED) suit.[142]

1. Common Law Remedies

Tanya Gersh successfully brought one such civil suit against Andrew Anglin, the publisher of an alt-right website, *The Daily Stormer*.[143] In 2016, Ms. Gersh, a realtor in Whitefish, Montana, agreed to work with Whitefish resident Sherry Spencer to sell Spencer's mixed-use commercial building.[144] Ms. Sherry Spencer is the mother of a white supremacist, Richard Spencer.[145] Richard Spencer gained notoriety after the 2016 presidential election when a video captured him saying "Hail Trump! Hail our people! Hail victory."[146] After years of discontent with Richard Spencer's behavior, members of the Whitefish community were outraged after

139. *See* BRANNON & HOLMES, *supra* note 124, at 30 ("[I]n 2018, the push to reform Section 230 gained further momentum in Congress. Twenty-six bills in the 116th Congress would have amended Section 230.").

140. Betuel, *supra* note 34.

141. MacAllister, *supra* note 58, at 2479.

142. *Id.*

143. Gersh v. Anglin, 353 F. Supp. 3d 958, 962–63 (D. Mont. 2018); Aaron Bolton, *Neo-Nazi Publisher Ordered to Pay $14 Million in Troll Storm Lawsuit*, MONT. PUB. RADIO (Aug. 8, 2019, 5:38 PM), https://www.mtpr.org/montana-news/2019-08-08/neo-nazi-publisher-ordered-to-pay-14-million-in-troll-storm-lawsuit [https://perma.cc/7J7U-GEJK].

144. *Tanya Gersh v. Andrew Anglin*, S. POVERTY L. CTR., https://www.splcenter.org/seeking-justice/case-docket/tanya-gersh-v-andrew-anglin [https://perma.cc/D3FZ-NS7R] (last visited Apr. 29, 2022) [hereinafter *Tanya Gersh*].

145. *Id.*

146. *Id.*

the release of this video.[147] In turn, members considered protesting outside of the Spencer-owned building.[148]

Ms. Spencer called Ms. Gersh, one of the few Jewish members of Whitefish, for advice after learning about the discontent within the community.[149] Ms. Spencer agreed to sell the building with help from Ms. Gersh, but Ms. Spencer ultimately decided against the sale and began posting online that she was pressured by Ms. Gersh into selling her property.[150] Mr. Anglin, a friend of Richard Spencer, discovered the story and began publishing news articles on his website.[151] Mr. Anglin attacked Ms. Gersh and published Ms. Gersh's phone numbers, email addresses, and social media profiles, as well as Gersh's husband and twelve-year-old son's personally identifiable information.[152]

In bringing her suit, Ms. Gersh relied on an invasion of privacy theory, an IIED theory, and Montana's Anti-Intimidation Act that protects against harassment, threats, and intimidation when one is attempting to exercise a legally protected right.[153] She was awarded over $14 million in compensatory and punitive damages.[154] Yet, the ability of other doxing victims to replicate Ms. Gersh's success is not guaranteed.

Ms. Gersh was able to succeed under a tort theory for a few unique reasons. For one, Ms. Gersh was able to point to a singular doxer, Mr. Anglin, who caused her harm and was clearly the proper defendant. He not only was the person that originally posted her personally identifiable information, but Mr. Anglin also called upon his readers to: "Just make your opinions known. Tell them you are sickened by their Jew agenda," and "hey—if you're in the area, maybe you should stop by and tell her in person what you think of her actions."[155] For many other victims, their cases of doxing may not involve instances of such explicit requests for action from a singular person. Rather, the doxer could just post the person's information and allow for an implied request for action from other "conspirators." Such a scenario would raise the complicated threshold question of who could be held liable in a tort suit, which was not present in Ms. Gersh's case.

Even if the victim could find a viable defendant, the victim would then need to prove the case on the merits of the tort claims, which may be difficult for a victim to do. If the doxer simply posted true information,

147. *Id.*
148. *Id.*
149. *Id.*
150. *Tanya Gersh*, *supra* note 144.
151. *Id.*
152. Gersh v. Anglin, 353 F. Supp. 3d 958, 962 (D. Mont. 2018).
153. *Id.* at 963; MONT. CODE ANN. § 27-1-503(2) (2021).
154. *Tanya Gersh*, *supra* note 144.
155. *Id.*

such as a victim's home address, a defamation suit would fail.[156] For an IIED suit to succeed, the victim would have to show that the defendant's conduct was outrageous or extreme.[157] The requirement of outrageous conduct is a high bar.[158] Ms. Gersh was able to easily pass this bar because "Anglin assisted, encouraged, and ratified a vicious campaign of anti-Semitic harassment against her and her family."[159] Comparatively, it is not obvious that a judge or a jury would view the mere posting of personally identifiable information as sufficiently outrageous. This hurdle could ultimately prove fatal to a victim's IIED suit.

It is likely that a doxing victim would need a severe case—one comparable to Ms. Gersh's—to prevail under tort law. It is doubtful that simply having personally identifiable information posted online would be sufficient for a victim to prevail under a tort law theory; yet, this is a common mode of doxing. Consequently, even though victims have these tort remedies available, there is still a need for specific doxing legislation because tort-based litigation will not often provide a viable solution for doxing victims.

2. Doxing Specific State Legislation

States have utilized various approaches when attempting to regulate doxing.[160] States have either strengthened pre-existing cyber-stalking laws to include doxing[161] or pursued specific anti-doxing legislation.[162] The categories of existing state-level anti-doxing legislation include statutes aimed at protecting groups of people such as law enforcement, judges,[163] or heath care workers;[164] general civil doxing statutes;[165] and

156. MacAllister, *supra* note 58, at 2479.

157. *See* Snyder v. Phelps, 562 U.S. 443, 451 (2011) (stating that to succeed in an IIED under Maryland law, a plaintiff must prove "the defendant intentionally or recklessly engaged in extreme and outrageous conduct that caused the plaintiff to suffer severe emotional distress.").

158. MacAllister, *supra* note 58, at 2479.

159. Gersh v. Anglin, 353 F. Supp. 3d 958, 970 (D. Mont. 2018).

160. Betuel, *supra* note 34.

161. *Id.*

162. *Id.*

163. *See* Jon Fingas, *New Jersey Law Bars Doxxing Campaigns Against Judges, Prosecutors and Police*, ENGADGET (Nov. 22, 2020), https://www.engadget.com/new-jersey-daniels-law-anti-doxxing-203258884.html [https://perma.cc/EZ58-TJTT] ("Governor Phil Murphy has signed Daniel's Law, a measure barring the publication (primarily on the internet) of home addresses and unlisted phone numbers for judges, prosecutors and law enforcement officers. It's named after Daniel Anderl, the son of Judge Esther Salas. A man murdered Daniel and injured his father after finding Judge Salas' address online.").

164. Betuel, *supra* note 34.

165. *E.g.*, A.B. 296, 2021 Leg., 81st Sess. (Nev. 2021) (enacted) (allowing a victim of doxing in Nevada to bring a civil action to recover damages).

criminal statutes.[166]

While legislation of any kind is a step in the right direction, there are a few overarching challenges with state legislation—both civil and criminal. For any state-based civil statutes, jurisdiction provides an initial challenge.[167] To bring a claim under state law in court,[168] the court would need to have personal jurisdiction over the doxer. In many instances, "getting" this jurisdiction could prove difficult for the victim because the doxer can use the Internet to dox from any location and any state.[169] It is inevitable that many doxing victims will seek cases against individuals who do not reside in their home state. To obtain jurisdiction over a nonresident in a civil case, the doxing victim would need to show that the defendant's action—doxing over the Internet—amounts to constitutionally minimum contacts with the victim's home state.[170]

The answer to this jurisdictional question would ultimately turn on what information the doxer posted and how strongly it relates to the victim's home state.[171] One court found minimum contacts existed when the doxer tweeted the victim's physical address in the forum state of Michigan, because the court viewed this as a plausible attempt "to pique Michiganders' interest with her tweet."[172] The court also noted that Michiganders were the ones most readily able to visit the residence.[173] However, the court acknowledged that "not . . . all doxing amounts to constitutionally minimum contacts," especially when the post has little relation to the forum state.[174]

This distinction is concerning because it favors attacks where doxers post information that can elicit a local response. Yet, many doxers may not post a home address and instead opt for email addresses or cell phone

166. *See, e.g.*, ARIZ. REV. STAT. ANN. § 13-2916.A. (2021) ("It is unlawful for a person to knowingly terrify, intimidate, threaten or harass a specific person or persons by doing any of the following: . . . 4. Without the person's consent and for the purpose of imminently causing the person unwanted physical contact, injury or harassment by a third party, use an electronic communication device to electronically distribute, publish, . . . or make available for downloading the person's personal identifying information, including a digital image of the person, and the use does in fact incite or produce that unwanted physical contact, injury or harassment.").

167. For a full discussion of finding personal jurisdiction in a social media case, *see* Ellen Smith Yost, *Tweet, Post, Share . . . Get Haled into Court? Calder Minimum Contacts Analysis in Social Media Defamation Cases*, 73 SMU L. REV. 693 *passim* (2020).

168. This is true for both state courts and federal courts sitting under diversity jurisdiction. *See id.* at 695.

169. *Id.*

170. Vangheluwe v. Got News, LLC, 365 F. Supp. 3d 850, 852 (E.D. Mich. 2019).

171. *See id.* at 857 (stating that a defamatory post on social media is insufficient for minimum contacts and that "the poster's conduct must have involved the plaintiff's state in some additional way").

172. *Id.* at 860.

173. *Id.*

174. *Id.* at 860–61.

numbers.[175] Such information is less connected to one's home state but can lead to just as harmful consequences and harassment for the victim. Ultimately, the personal jurisdiction requirement for a civil statute will leave doxing victims wondering whether they will have access to recourse or may even preclude victims from successfully suing. Such uncertainty against a tactic that can cause such harm should be unacceptable.

A state statute criminalizing doxing would also present some jurisdictional challenges for a non-resident defendant, but arguably fewer. Instead of the "minimum contacts" analysis required for a civil suit, jurisdiction over a non-resident defendant in a criminal case focuses on the "intent of the defendant and the effects within the forum state."[176] To obtain criminal jurisdiction over an out-of-state doxer, the state[177] would typically need to show: "(1) an act occurring outside the state, which is (2) intended to produce detrimental effects within the state, and (3) is the cause of detrimental effects within the state."[178] The usual difficulty for the prosecution is showing the defendant *intended* to cause harm within the forum state.[179] In instances of doxing, a defendant could try to argue they did not necessarily intend harm in the forum state. However, a foundational aspect of doxing is the intent to cause some level of harm to the target. The target, in turn, resides in a specific state. If one intends to harm a specific individual who resides in a specific state, there is an inextricable intent to cause harm in that state.[180] Because of this connection, a court is likely to consider the intent element sufficiently satisfied, and the act of doxing would likely subject the doxer to a state criminal court's jurisdiction.

Nonetheless, there is one major flaw with state-by-state legislation. Doxing happens all over the country; however, a victim only has access to legal recourse if their forum state has an anti-doxing statute. While there is growing concern around the practice, citizens in thirty-nine states

175. *See* Park, *supra* note 41 (stating that in a 2017 NYU study of 5,500 doxing cases, 90% of cases included victim's address, 61% included a phone number, and 53% included an email address).

176. TERRENCE BERG, STATE CRIMINAL JURISDICTION IN CYBERSPACE: IS THERE A SHERIFF ON THE ELECTRONIC FRONTIER? 2 (2007), http://euro.ecom.cmu.edu/program/law/08-732/Crime/StateCriminalJurisdictionBerg.pdf [https://perma.cc/UN4V-4DM2].

177. In 1911, the Supreme Court first recognized that states could exercise criminal jurisdiction over acts committed outside its territorial bounds where the perpetrator intended to produce, and actually produced, detrimental effects within the state. *See* Strassheim v. Daily, 221 U.S. 280, 285 (1911). Since that decision, numerous states have adopted statutes codifying this type of extraterritorial criminal jurisdiction over defendants. *See* BERG, *supra* note 176 (listing 22 states that had adopted jurisdictional statutes by 2007).

178. BERG, *supra* note 176.

179. *Id.*

180. *See* State v. Amoroso, 975 P.2d 505, 509 (Utah Ct. App. 1999) (finding jurisdiction in part because an out-of-state retailer supplied beer to minors in the forum state).

are currently without specific protections.[181] In such instances, victims must bring makeshift tort claims, which as previously discussed, are not guaranteed to succeed.[182] Legislation on the federal level would swiftly ensure that Americans are protected against this practice, irrespective of where they reside.

C. *Federal Regulation*

Federal legislation is the optimal solution to regulate doxing. A piece of federal legislation that regulates doxing would provide federal courts jurisdiction over such cases. It would obviate any jurisdictional concerns that may be present with state statutes. Next, if the statute were criminal, it would constitute an exception to CDA Section 230 immunity.[183] Section 230 states that "[n]othing in this section shall be construed to impair the enforcement of . . . any other Federal criminal statute."[184] The Justice Department has relied on this exception in the past. In 2018, the Justice Department successfully prosecuted Backpage.com and its corporate entities for conspiracy to engage in money laundering.[185] Similarly, a federal statute criminalizing doxing could provide prosecutors a way to go after social media sites without waiting for amendments to Section 230. This possibility requires a federal criminal statute, because courts have held that this exception does not apply to state criminal statutes or civil suits based on federal criminal laws.[186]

Despite these benefits, no federal statute specifically addresses doxing. Nevertheless, some have argued that the government could utilize the Interstate Communications Statute (ICS) and the Interstate Stalking Statute (ISS) as a workaround to prosecute doxers.[187] The ICS criminalizes "any communication containing any threat to kidnap any person or any threat to injure the person of another."[188] Comparatively, the ISS prevents a person from engaging in a course of conduct on the internet with the intent to "kill, injure, harass, intimidate, or place under surveillance" another person, and that conduct must place that person in "reasonable fear of death or serious bodily injury" or cause "substantial emotional distress."[189]

By their terms, these statutes are written broadly enough to include some instances of doxing, but each statute was not crafted with doxing's

181. Betuel, *supra* note 34.
182. *See* discussion *infra* Section III.B.1.
183. BRANNON & HOLMES, *supra* note 124, at 24.
184. 47 U.S.C. § 230(c)(1) (2011).
185. BRANNON & HOLMES, *supra* note 124, at 25 n.250.
186. *Id.* at 25.
187. MacAllister, *supra* note 58, at 2470, 2474.
188. 18 U.S.C. § 875(c) (2021).
189. *Id.* § 2261A(2).

unique features in mind. For that reason, there would be challenges with enforcement. The ICS requires the user to issue a "threat to kidnap" or "threat to injure."[190] Though the statute does not define what constitutes a threat, at least one Justice has used the term's plain meaning and stated it is "an expression of an intention to inflict evil, injury, or damage on another."[191] In the doxing realm, such a requirement could prove fatal to a suit under the ICS, because doxers may only post personally identifiable information and not make an explicit threat of violence.[192] While some would consider sharing personally identifiable information a threat in and of itself, it is not clear that, given this precedent and specific statutory language, courts would consider the release of personal information "an expression of intention to inflict" injury under the ICS without explicit mentions of violence.[193]

The ISS has flaws when applied to doxing as well. Notably, the ISS requires the perpetrator to engage in a "course of conduct."[194] A course of conduct is defined as "a pattern of conduct composed of two or more acts, evidencing a continuity of purpose."[195] Again, since doxing typically involves multiple actors taking on different roles,[196] a doxer could evade prosecution because they posted personally identifiable information only once. Being able to avoid liability because of a technicality like this seems unjust, especially when a single post of personally identifiable information could cause just as much harm as a course of conduct. These flaws indicate the current federal scheme is insufficient to protect individuals against doxing. A specific federal doxing statute would provide much needed coverage.

III. A SOLUTION: A MODIFIED INTERSTATE DOXXING PREVENTION ACT

At present, there are a few pieces of proposed federal legislation that concern doxing, but Congresswoman Katherine Clark's proposal provides a valuable foundation for a federal statute.[197] After facing a doxing and swatting campaign herself, Congresswoman Clark proposed anti-

190. *Id.* § 875(c).

191. Elonis v. United States, 575 U.S. 723, 744 (2015) (Alito, J., concurring in part, dissenting in part).

192. MacAllister, *supra* note 58, at 2470.

193. *Elonis*, 575 U.S. at 744.

194. 18 U.S.C. § 2261A(2) (2020).

195. *Id.* § 2266(2).

196. MacAllister, *supra* note 58, at 2474.

197. *Compare* A Bill to Protect Federal Judges, Federal Prosecutors, and Federal Law Enforcement Officers from Violence and Doxing, S. 2247, 117th Cong. (2021) (protecting federal judges, prosecutors, and law enforcement from doxing), *with* Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. (2016) (containing no such specific limitation).

doxing legislation in 2016.[198] Titled as the "Interstate Doxxing Prevention Act" (IDPA), the statute would create criminal liability, and the option for civil liability, when individuals have their personally identifiable information published when the publisher intends harm.[199] Despite its strengths, as the IDPA presently stands, it is flawed. Utilizing the IDPA as a starting point, Section A, Part III, of this Article proposes modifications to create an anti-doxing statute that is likely to survive a First Amendment challenge.

A. *Proposals for the Interstate Doxxing Prevention Act*

At present, the Act states:

> (a) Prohibition—Whoever, with the intent to threaten, intimidate, harass, stalk, or facilitate another to threaten, intimidate, harass, or stalk, uses the mail or any facility or means of interstate or foreign commerce to knowingly publish the personally identifiable information of another person, and as a result of that publication places that person in reasonable fear of the death of or serious bodily injury to—
>
> (1) that person;
>
> (2) an immediate family member of that person; or
>
> (3) an intimate partner of that person,
>
> shall be subject to the criminal penalty and the civil liability provided by this section.[200]

The bill defines "publish" as "to circulate, deliver, distribute, disseminate, transmit, or otherwise make available to another person."[201] The IDPA defines "personally identifiable information" as:

> (a) any information that can be used to distinguish or trace an individual's identity, such as name, prior legal name, alias, mother's maiden name, social security number, date or place of birth, address, phone number, or biometric data;
>
> (b) any information that is linked or linkable to an individual, such as medical, financial, education, consumer, or employment information, data, or records; or
>
> (c) any other sensitive private information that is linked or linkable to a specific identifiable individual, such as gender identity, sexual orientation, or any sexually explicit visual

198. Calabro, *supra* note 46, at 56, 66.
199. Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. (2016).
200. *Id.* § 2.
201. *Id.*

> depiction of a person described in clause (1), (2), or (3) of subsection (a).[202]

Finally, this bill provides for one carve-out. It states, "[t]his section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or political subdivision of a State, or of an intelligence agency of the United States."[203]

While the IDPA has some benefits, it is a content-based regulation. It must be crafted in a way that is narrowly tailored and restricts the least amount of speech, so as not to be struck down as unconstitutional.[204] To ensure that the IDPA is sufficiently tailored, this Article proposes amendments to the prohibition section, the addition of two more carve-outs, and an explicit statement the IDPA does not apply to constitutionally protected activity.

The IDPA should be amended as follows,[205] with the proposals in italics:

> (b) Prohibition—Whoever,
>
> > (i) with the intent to threaten, intimidate, harass, stalk, or facilitate another to threaten, intimidate, harass, or stalk, uses the mail or any facility or means of interstate or foreign commerce to knowingly publish personally identifiable information of another person *without consent*;
> >
> > (ii) and as a result of that publication *would cause a reasonable person to suffer significant economic injury or severe mental anguish, to fear serious bodily injury, death, or stalking, or to fear that serious bodily injury or death will be inflicted on—*
> >
> > > (1) an immediate family member of that person; or
> > >
> > > (2) an intimate partner of that person,
>
> shall be subject to the criminal penalty and the civil liability provided by this section.

---

202. *Id.*

203. *Id.*

204. City of Los Angeles v. Alameda Books, Inc., 535 U.S. 425, 434 (2002).

205. These amendments were inspired by a recent bill introduced in Nebraska's legislature by Senator Adam Morfeld, which the Anti-Defamation League help draft, and the NCP statutes from Vermont and Minnesota. *See* L.B. 227, 107th Leg., 1st Sess. (Neb. 2021); VT. STAT. ANN. tit. 13, § 2606 (2019); MINN. STAT. § 617.261 (2021).

Next, the following carve-outs should be added:

> *Exclusions: This section shall not apply to:*
> *(1) Disclosures of personally identifiable information that constitute a matter of public concern or are part of a newsworthy event;*
>
> *(2) Disclosures of only a person's name, prior legal name, alias, mother's maiden name. Additional personally identifiable information beyond one person's name, prior legal name, alias, mother's maiden name must be included in the publication for this section to apply.*
>
> Lastly, the following clause should be added: *The Legislature does not intend the Interstate Doxxing Prevention Act to allow prosecution for constitutionally protected activity.*

B. *The Amended Interstate Doxxing Prevent Act Would Likely Survive a First Amendment Challenge*

With these additions, the IDPA would likely survive strict scrutiny and a constitutional challenge. Under strict scrutiny, the government would first need to establish a compelling government interest in regulating doxing.[206] In articulating a compelling interest, the government should emphasize that doxing involves speech on private matters under the IDPA. In turn, this will make it easier for the statute to pass strict scrutiny because speech on purely private matters tends to carry less weight in the strict scrutiny analysis.[207]

In general, while personally identifiable information has varying degrees of publicness when a doxer decides to release this information during a doxing campaign, it is not going to be a matter of public concern. Indeed, doxers are often doxing to *reveal* a formerly anonymous person's identity.[208] They are posting a private individual's information so other Internet users will learn who the person is and related facts about them such as age, employment location, and financial information. The information is then curated and weaponized so the masses can easily access the victim in real life. The information is not "fairly considered as relating to any matter of political, social, or other concern to the community."[209] Rather, it is truly a public disclosure of a private individual's information.

206. Brown v. Ent. Merchs. Ass'n, 564 U.S. 786, 799 (2011).
207. State v. VanBuren, 214 A.3d 791, 808 (Vt. 2019).
208. Garber, *supra* note 35.
209. Snyder v. Phelps, 562 U.S. 443, 453 (2011).

In evaluating Tanya Gersh's suit, the court acknowledged this reality and was receptive to the notion that her doxer's speech could be fairly construed as a matter of strictly private concern.[210] The amended IDPA also ensures that it does not proscribe speech that is connected to matters of public concern. If the publicly identifiable information was of public concern, the statute explicitly provides for a public interest exception. This should be sufficient for a court to consider the amended IDPA as only proscribing speech on purely private matters.

A compelling interest in regulating doxing is present because doxing substantially invades the victim's privacy, leads to substantive harms, and is rooted in the intentional creation of harassment and threats. States have regularly protected citizens against unreasonable invasions of privacy. This protection has included creating a right of action for "publicity given to private life."[211] Similarly, doxing creates unfettered intrusions into victims' private lives through the public exposure of personally identifiable information. Incessant phone calls, messages, emails, letters, social media comments, or home visits then follow the victim and possibly the victim's family members.[212] In many ways, doxing is the modern way to take away the ability of victims to retreat into the sanctity of one's home. It eviscerates any notion of anonymity and privacy the victim once had, and it is done entirely without the victim's consent. Doxing victims are truly dragged into the spotlight against their will. In such scenarios, courts have historically permitted the protection of the individual's privacy rights, and thus the government should be permitted to do so here.[213]

Doxing also leads to considerable injuries. Posting personally identifiable information subjects the target to death threats, stalking, swatting, constant harassment, and severe emotional distress.[214] There is no foreseeable endpoint to the harassment either—once the personally identifiable information is released, it becomes very difficult to "put the genie back in the bottle." Furthermore, victims can experience job loss, and the practice can prevent them from obtaining employment down the line.[215] Similar harms have been used to justify other statutes against First

210. Gersh v. Anglin, 353 F. Supp. 3d 958, 966 (D. Mont. 2018).

211. *VanBuren*, 214 A.3d at 802.

212. Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1098 (9th Cir. 2009); *see Gersh*, 353 F. Supp. 3d at 963 (noting that "[w]hen Gersh filed her Complaint in the spring of 2017, she and her family had received more than 700 disparaging and/or threatening messages").

213. *See* RESTATEMENT (SECOND) OF TORTS § 652A cmt. a (AM. L. INST. 1977) (describing how invasion of privacy claims are all rooted in an "interference with the interest of the individual in leading, to some reasonable extent, a secluded and private life, free from the prying eyes, ears and publications of others").

214. MacAllister, *supra* note 58, at 2453; Betuel, *supra* note 34.

215. *Cancel Culture*, *supra* note 26.

Amendment challenges, and these injuries should also be sufficient for doxing.[216]

Lastly, doxers intend to inflict harm and cause fear with their actions. Causing injury is foundational to the tactic. Doxers know that in posting the personally identifiable information, the target will either endure actual threats from people who see the post, or nevertheless face the distressing realization that the Internet now has access to their phone number and where they live. The government should be able to protect its citizens from this type of intentional creation of fear. After all, true threats are exempt from First Amendment protections to "protect[] individuals from the fear of violence, from the disruption that fear engenders, and from the possibility that the threatened violence will occur."[217] This reasoning also applies to doxing. In sum, the invasions of privacy, substantial harm, and the malicious and threatening nature of doxing constitutes a compelling government interest that justifies regulation.

After articulating a compelling interest, the government would need to show that the IDPA is "narrowly tailored" and uses the least restrictive means to regulate the speech.[218] In looking for narrowly tailored statutes in other contexts, courts have considered: (1) whether the statute provides clear definitions; (2) the applicable mens rea; and (3) whether there are statutory carve-outs.[219] The amended IDPA has each of these features and is narrowly tailored to the harms of doxing.

To start, the IDPA precisely defines what constitutes "personally identifiable information" and "publishing." A clear definition of these terms is important because it decreases the risk of sweeping in constitutionally protected speech. Next, the IDPA has a malicious intent requirement and requires a knowing mens rea. It only attaches liability when the doxer has the specific intent to harm, harass, intimidate, or threaten. Further, it criminalizes doxing when the doxer *knowingly* publishes personally identifiable information without the target's consent. Requiring a knowing mens rea and the specific intent to harm creates a high standard. It means the statute will not cover negligent, or even reckless publications, and ensures that the statute only covers a narrow category of speech. Courts have been receptive to upholding statutes criminalizing protected speech where there is a knowing mens rea and specific intent to harm requirement.[220] Though courts could accept a lower mens rea—like recklessness—this

216. State v. Katz, 179 N.E.3d 431, 459 (Ind. 2022).

217. R.A.V. v. City of St. Paul, 505 U.S. 377, 388 (1991).

218. City of Los Angeles v. Alameda Books, Inc., 535 U.S. 425, 455 (2002).

219. State v. VanBuren, 214 A.3d 791, 811 (Vt. 2019); State v. Casillas, 952 N.W.2d 629, 643–44 (Minn. 2020); *Katz*, 179 N.E.3d at 459.

220. *See VanBuren*, 214 A.3d at 811–12; *Casillas*, 952 N.W.2d at 643; *Katz*, 179 N.E.3d at 459–60.

higher standard follows recent jurisprudence and gives the amended IDPA the best chance to pass constitutional muster.

The IDPA with its additional carve-outs tailors the applicability of the Act and guarantees that it only targets speech in accord with First Amendment jurisprudence. The original carve-out exempted investigative or intelligence activities of law enforcement.[221] This is beneficial because law enforcement often enlists the public to identify individuals suspected of crimes. For example, the FBI recently requested the public's assistance in identifying individuals captured on videos who attended the January 6th U.S. Capitol riot.[222] The IDPA would explicitly protect the public's assistance with this type of law enforcement identification request.

As amended, the IDPA also contains a "newsworthiness" exception, that would permit the publishing of personally identifiable information when it of "public concern." This carve-out is essential. Matters of public concern are at the heart of the First Amendment.[223] A statute that limits public commentary on public issues would run the very real risk of not surviving a First Amendment challenge. Courts have proven receptive to upholding statutes criminalizing protected speech where there is a public concern exception.[224]

One may argue that this carve-out is too broad; whether something is of "public concern" may vary in the matter of days in our viral, Internet-based, society. For example, when Amy Cooper was initially doxed, her story may not have been of public concern. But, days later, it was a national news story. Courts would have to evaluate whether the information was a matter of public concern at the time of its publication. This may result in excluding some doxing victims from coverage. Nevertheless, this carve-out is likely a necessary provision for courts to uphold the IDPA and afford victims a much-needed remedy for doxing.

This newsworthy carve-out would also protect journalists who may release names and addresses when covering stories.[225] The Court has noted in *Cox Broadcasting Corp. v. Cohn* that reporters cannot be made liable for publishing names in the public record.[226] This carve-out assures that the IDPA is in line with this holding. Moreover, protection for journalists is important now more than ever. Reporters have recently come

221. Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. § 2 (2016).

222. *See U.S. Capitol Violence*, FBI MOST WANTED, https://www.fbi.gov/wanted/capitol-violence [https://perma.cc/GJ79-6D9G] (compiling videos and over 400 pictures of attendees at the January 6th riot that the FBI are requesting assistance in identifying) (last visited May 18, 2023).

223. Snyder v. Phelps, 562 U.S. 443, 451–52 (2011).

224. *VanBuren*, 214 A.3d at 791; *Casillas*, 952 N.W.2d at 643.

225. *Casillas*, 952 N.W.2d at 643.

226. Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 491 (1975).

under attack in the doxing debate.[227] Yet, journalists are essential to free speech and press. This carve-out would guarantee that journalists are not precluded from adequately doing their job.

Lastly, the amended IDPA makes clear it does not infringe upon other constitutional activity. This statement acknowledges that the IDPA may have to give way to overriding First Amendment values. One such scenario is instances of public figures and doxing.[228] Where a doxing case is premised on the release of personally identifiable information of a public figure, it is unlikely that a suit or criminal prosecution would proceed. This is because First Amendment jurisprudence has repeatedly noted that public figures are individuals "intimately involved in the resolution of important public questions or, by reason of their fame, shape events in areas of concern to society at large."[229] Therefore, they are not afforded the same protections as private individuals.[230] In such instances, it is more likely that doxing of a public figure would constitute "public concern." In conjunction with the public concern carve-out, this additional statement makes clear that the IDPA does not infringe upon First Amendment jurisprudence surrounding public figures. This also makes certain that the IDPA is narrowly tailored.

These clear definitions, mens rea, and statutory carve-outs all ensure that the IDPA is narrowly tailored. Given the compelling government interest, the IDPA is likely to survive strict scrutiny.

C. *The Amended Interstate Doxing Prevention Act Has Additional Strengths That Address Doxing's Unique Features*

The amended IDPA has distinctive aspects which make it a valuable tool to combat doxing. First, the IDPA only proscribes speech when the doxer knowingly publishes the information with the *intent* "to threaten, intimidate, harass, stalk."[231] In conjunction with the public concern carve-out, this malicious intent requirement would prevent the prosecution of truly good faith awareness campaigns.

Additionally, the IDPA contains "facilitation" language. Under this proposed statute, liability will attach if one "facilitate[s] another to threaten, intimidate, harass, or stalk."[232] This language is critical because it will ensure prosecutors can go after some of the "conspirator" doxers—the participants that may assist in the campaign but are not the initial

227. Ariel Zilber, *Taylor Lorenz Slammed for 'Doxxing' 'Libs of TikTok' Creator*, N.Y. POST (Apr. 19, 2022, 11:05 AM), https://nypost.com/2022/04/19/taylor-lorenz-blasted-for-doxxing-libs-of-tiktok-creator/ [https://perma.cc/DW8G-7T8F].

228. Hustler Mag., Inc. v. Falwell, 485 U.S. 46, 51 (1988).

229. *Id.*

230. *Id.* at 51–53.

231. Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. § 2 (2016).

232. *Id.*

poster. Having a way to address the multiple actors in a doxing crusade is crucial, and the IDPA has language to that effect.

This language would also likely create a route for prosecutors to pursue the social media companies that permit doxing on their sites. Since the IDPA is a federal criminal statute, CDA Section 230 liability would not apply. Prosecutors could then use this basis to argue that the site facilitated another to threaten, intimate, harass, or stalk. In turn, the IDPA could prove valuable in pressuring social media companies to effectively regulate doxing on their own.

The IDPA's definition of personally identifiable information is advantageous because it covers the information doxers most often release. Academic studies that focus on doxing and compile quantitative data on the subject are rare.[233] But, in one of the only available studies, researchers found that of the 5,500 online files associated with doxing, 90% included the victim's address, 61% included a phone number, 53% included an email address, 33% included a date of birth, and 50% included information about the target's family members.[234] Though less common, the doxing files contained credit card numbers (4.3%) and social security numbers (2.6%) at times.[235] The IDPA definition of personally identifiable information reflects the research and covers phone numbers, addresses, date, or place of birth. The definition also goes beyond this and covers more information that doxers could release, such as biometric data. This will allow the statute to adequately respond to advancements in technology, such as facial recognition technology, which could influence the type of information doxers release in the future. Importantly, the IDPA's definition of personally identifiable information covers "employment information." This is significant because doxers are more frequently publishing the victim's place of employment. Indeed, TikTok videos regularly include such information.[236] The IDPA adequately accounts for this development.

The IDPA no longer requires that the publication of personally identifiable information must place a person in "reasonable fear of the death

233. *See* Briony Anderson & Mark A. Wood, *Doxing: A Scoping Review and Typology*, *in* THE EMERALD INTERNATIONAL HANDBOOK OF TECHNOLOGY-FACILITATED VIOLENCE AND ABUSE 205, 208 (Jane Bailey et al. eds., 2021).

234. Peter Snyder et al., *Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing*, *in* PROCEEDINGS OF THE 2017 INTERNET MEASUREMENT CONFERENCE 432, 434, 437–38 (2017).

235. *Id.* at 438.

236. *See, e.g.*, Danesh (@thatdaneshguy), TIKTOK (Jan. 30, 2022), https://www.tiktok.com/@thatdaneshguy/video/7058919000859856174?is_from_webapp=1&sender_device=pc&web_id6947444569463358982 [https://perma.cc/2VZA-TXN3] ("Hello Roger Miller, director of golf and recreation in the city of Coronado, San Diego. Oof, this one's going to be messy.").

of or serious bodily injury."[237] This requirement mandated a high level of harm and thus ran the risk of excluding many victims who instead suffer from severe emotional distress, reputational or financial harms, or job loss. As amended, the IDPA permits liability when a person suffers significant economic injury, severe mental anguish, fear of death, bodily harm, or stalking. This amendment affords greater protection to more people.

Finally, the IDPA no longer permits liability for Internet users who only post an individual's name. This added carve-out is valuable because attaching criminal liability for only posting one's name creates a very low bar. It could capture too much speech. A full name on the Internet may serve as a key to unlock other personally identifiable information, but the legislature must make difficult decisions about the point at which liability attaches. The mere posting of one's name is too low of a bar, and the amended IDPA acknowledges this.

CONCLUSION

In considering the application of unchanging constitutional principles to new and rapidly evolving technology, courts should proceed with caution. We should make every effort to understand new technology. We should consider the possibility that important societal implications of developing technology may become apparent only with time. We should not jump to the conclusion that new technology is fundamentally the same as some older thing with which we are familiar. We should also not hastily dismiss the judgment of legislators, who may be in a better position than we are to assess the implications of new technology.[238]

Doxing is a harmful tactic. It is used to harass and inflict severe emotional distress, and it has the potential to stifle the free flow of thought. The time has now come to regulate doxing and the best way to do so is through a federal statute. The suggested amendments to the IDPA provide legislators with an example of legislation that was narrowly drafted to pass a First Amendment challenge. Doxing-specific legislation is needed so victims like Damon Young and Brianna Wu are not left without protection.

The time is now for Congress to act. Doxing has entered the mainstream's consciousness and the current legal framework is not equipped to protect doxing victims. Moreover, doxing will likely surge in popularity in the coming years, because social media sites like TikTok, which

237. Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. § 2 (2016).

238. Brown v. Ent. Merchs. Ass'n, 564 U.S. 786, 806 (2011) (Alito, J., dissenting).

has quickly become the most popular web domain,[239] have countless pages that promote doxing-like behaviors. Given the malleability of the tactic, which can be used against individuals on either side of the political spectrum, there should be a viable chance at securing bipartisan support for federal doxing legislation.

239. Johan Moreno, *TikTok Surpasses Google, Facebook as World's Most Popular Web Domain*, FORBES (Dec. 29, 2021, 4:47 PM), https://www.forbes.com/sites/johanmoreno/2021/12/29/tiktok-surpasses-google-facebook-as-worlds-most-popular-web-destination/?sh=4b0ea2b643ef [https://perma.cc/PD3Y-BTZK].