# From the Message Board to the Front Door: Addressing the Offline Consequences of Race- and Gender-Based Doxxing and Swatting

*"If you've never been on the receiving end of a viral Internet hate mob, it's hard to convey the confluence of galloping adrenaline and roaring dread."*[1]

## I. INTRODUCTION

At ten o'clock on a Sunday night, while her children were in bed, flashing police lights suddenly flooded Congresswoman Katherine Clark's home.[2] Clark looked outside and saw police cruisers barricading both ends of her street and officers with "long guns" facing her home.[3] The officers informed Clark that an anonymous tipster with a digitized voice had reported that Clark's home was under attack by an "active shooter."[4] As a vocal activist against cyber harassment, Clark knew that she had fallen victim to "swatting"—an aggressive form of online abuse in which perpetrators falsely lure police into dispatching heavily armed tactical units to victims' homes.[5]

Swatting often emanates from "doxxing," or the public release of an individual's personal information or documents on the Internet.[6] Doxxers and swatters exploit the anonymity and instantaneousness of the Internet to intimidate and silence victims both online and offline.[7] This social and emotional harm is compounded by the fact that doxxing and swatting disproportionately affect women and people of color, and are often coupled

---

1. LINDY WEST, SHRILL: NOTES FROM A LOUD WOMAN 203 (2016).

2. *See* Ann Friedman, *Katherine Clark Is Taking on the Trolls*, ELLE (July 13, 2016), http://www.elle.com/culture/tech/a37728/katherine-clark-harassment-abuse-legislation/ [https://perma.cc/EY32-DE9N] (describing Clark's personal experience with swatting); Joshua Miller, *Police Swarm Katherine Clark's Home After Apparent Hoax*, BOS. GLOBE (Feb. 1, 2016), https://www.bostonglobe.com/metro/2016/02/01/cops-swarm-rep-katherine-clark-melrose-home-after-apparent-hoax/yqEpcpWmKtN6bOOAj8FZXJ/story.html (recounting scene of incident).

3. *See* Friedman, *supra* note 2 (describing officers' rifle-like guns).

4. *See id.* (detailing Clark's interaction with police).

5. *See id.*; Miller, *supra* note 2 (defining swatting).

6. *See* Patricia R. Recupero, Commentary, *New Technologies, New Problems, New Laws*, 44 J. AM. ACAD. PSYCHIATRY & L. 322, 325 (2016), http://jaapl.org/content/jaapl/44/3/322.full.pdf [https://perma.cc/X3TT-NG9V] (defining doxxing); Victoria McIntyre, Comment, *"Do(x) You Really Want to Hurt Me?": Adapting IIED as a Solution to Doxxing by Reshaping Intent*, 19 TUL. J. TECH. & INTELL. PROP. 111, 115 (2016) (positing doxxing leads to swatting).

7. *See* Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 64 (2009) [hereinafter Citron, *Cyber Civil Rights*] (describing social and emotional effects of online intimidation). Citron suggests that online harassment both "terrorize[s] victims" and "impair[s] [their] ability to participate in online and offline society as equals." *See id.*; *see also infra* Section II.A (explaining how Internet allows aggregation of online abuse).

with threats of physical and sexual violence.[8] The effects of these tactics permeate victims' offline lives, often inflicting irreparable emotional, professional, and physical harm onto already marginalized groups.[9]

The current lack of legal repercussions for doxxing and swatting further exacerbates the harmful effects of online harassment.[10] Many victims feel that law enforcement agencies do not take their harassment seriously, and that existing laws inadequately address their unique concerns as cyber victims.[11] As a result of this disconnect, victims' harassment goes unredressed, and harassers' abusive actions continue to go unchecked.[12] Nevertheless, emerging legislation addressing both swatting and doxxing provides a vital foundation for holding harassers accountable for their actions and reversing this trend of online abuse.[13]

8. *See* Citron, *Cyber Civil Rights*, *supra* note 7, at 64 (emphasizing frequent and intense harassment of women and people of color online). Citron describes how one group of online harassers doxxed a female blogger and doctored photos to depict her "head atop naked bodies" alongside graphic rape threats. *See id.* at 75-76 (detailing gendered nature of threats); *see also* Elle Hunt, *Online Harassment of Women at Risk of Becoming 'Established Norm', Study Finds*, GUARDIAN (Mar. 7, 2016), https://www.theguardian.com/lifeandstyle/2016/mar/08/online-harassment-of-women-at-risk-of-becoming-established-norm-study [https://perma.cc/JF2X-8M7S] (describing study finding younger women frequently targeted online).

9. *See* Citron, *Cyber Civil Rights*, *supra* note 7, at 86, 89 (highlighting psychological and economic impact of online harassment); *infra* Section II.A (discussing real-world implications of doxxing); *infra* Section II.B (detailing offline consequences of swatting).

10. *See* Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 402-03 (2009) [hereinafter Citron, *Expressive Value*] (highlighting infrequent police investigation of cyber harassment claims and light sentences for offenders); Bailey Roese, *Defamation, Humiliation, and Lost Reputations: Mitigating the Damage to Women Harassed Online*, 35 WOMEN'S RTS. L. REP. 123, 124-27 (2014) (summarizing ineffective lawsuits against Juicy Campus and AutoAdmit); *infra* Section II.D.1 (outlining barriers to holding online harassers legally accountable for their actions).

11. *See* Citron, *Expressive Value*, *supra* note 10, at 384-92, 395-404, 407-08 (discussing police underestimation of online harassment and cyber harassment's impact on women); Leigh Alexander, *Online Abuse: How Women Are Fighting Back*, GUARDIAN (Apr. 13, 2016), https://www.theguardian.com/technology/2016/apr/13/online-abuse-how-women-are-fighting-back [https://perma.cc/KDA2-QLNC] (noting prevalence of law enforcement's unfamiliarity with Internet forums); *see also* Elizabeth M. Jaffe, *Swatting: The New Cyberbullying Frontier After* Elonis v. United States, 64 DRAKE L. REV. 455, 457, 475-76 (2016) (explaining difficulty of proving "true threat" of cyber harassment); *infra* Section II.D.2 (examining law enforcement's inadequate understanding of cyber harassment).

12. *See* Citron, *Cyber Civil Rights*, *supra* note 7, at 83 (criticizing lack of social repercussions for online harassers). Citron suggests that online harassers' anonymity frees them from "social stigma for their abusive conduct," and enables them to harass victims without considering the emotional consequences of their actions. *See id.*; *see also* Jessica Valenti, *How the Web Became a Sexists' Paradise*, GUARDIAN (Apr. 5, 2007), https://www.theguardian.com/world/2007/apr/06/gender.blogging [https://perma.cc/5Z5U-XRAP] (suggesting Internet anonymity and misogyny create "gang-rape like mentality" online); *infra* Sections II.D.1-2 (highlighting lack of consequences for cyber harassers).

13. *See* J.D. Capelouto, *Meet the Congresswoman from Mass. Taking on Cyber Criminals*, BOSTON.COM (Sept. 29, 2016), https://www.boston.com/news/politics/2016/09/29/meet-the-congresswoman-from-mass-taking-on-cyber-criminals (describing Congresswoman Clark's anti-harassment legislation); *infra* Section II.E (detailing emerging legislation on doxxing and swatting); *see also* Jaffe, *supra* note 11, at 467-68 (outlining developing swatting legislation); Hannah Levintova, *This Congresswoman Has Plans to Stop Online Harassment*, MOTHER JONES (Sept. 15, 2016), http://www.motherjones.com/politics/2016/09/katherine-clark-fight-against-internet-trolls-gamergate [https://perma.cc/Q9Y3-BRE4] (tracking Congresswoman Clark's anti-harassment legislation).

This Note explores the broader social and emotional implications of doxxing and swatting, and analyzes how emerging legislation could help curtail online harassment.[14] This Note begins by examining how swatting and doxxing surpass typical free speech by tangibly interfering with victims' safety, livelihood, and mental health.[15] Specifically, this Note scrutinizes the gender- and race-based nature of doxxing and swatting, and demonstrates how these types of harassment suppress diverse perspectives both online and in social communities.[16] Moreover, this Note outlines the legal barriers to curtailing online harassment, as well as the inadequacy of current law enforcement policies surrounding cyber harassment.[17] In connection with those obstacles, this Note reviews proposed legislation that may alleviate harassment by both imposing legal penalties on harassers and encouraging expanded police training on cyber abuse.[18] Finally, this Note analyzes the prejudicial suppression of free speech that doxxing and swatting engender, and highlights the importance of deterring and preventing cyber harassment.[19]

## II. HISTORY

### *A. Overview of Doxxing*

Doxxing, shorthand for "dropping documents," is the public release of an individual's personal information.[20] Doxxers have developed a complex

14. *See infra* Part II (outlining catalysts and effects of online abuse, and possible legal solutions).

15. *See infra* Section II.A (discussing practical implications of doxxing and swatting); *see also* Citron, *Expressive Value*, *supra* note 10 at 381-82 (describing how harassment derailed law student's education and career); Jacqueline D. Lipton, *Combating Cyber-Victimization*, 26 BERKELEY TECH. L.J. 1103, 1104-05 (2011) (noting cyber harassment leads to physical harm); Matthew J. Enzweiler, Note, *Swatting Political Discourse: A Domestic Terrorism Threat*, 90 NOTRE DAME L. REV. 2001, 2038 (2015) (characterizing some swatting comparable to domestic terrorism); Sarah Jameson, Comment, *Cyberharassment: Striking a Balance Between Free Speech and Privacy*, 17 COMMLAW CONSPECTUS 231, 231-33 (2008) (discussing tragic death of teen girl after cyber harassment); Rex M. Shannon III, Comment, *Nightmare on Your Street: Moving Towards Justice for Innocent Victims of Wrong-Premises SWAT Raids*, 77 MISS. L.J. 669, 672-73 (2007) (discussing financial and emotional effects of unnecessary SWAT raids).

16. *See infra* Section II.C (exploring gender- and race-based motivations behind doxxing and swatting); *see also* Citron, *Expressive Value*, *supra* note 10, at 386 (noting threats constrain women's online and professional activities); Amanda Hess, *Why Women Aren't Welcome on the Internet*, PAC. STANDARD (Jan. 6, 2014), https://psmag.com/why-women-aren-t-welcome-on-the-internet-aa21fdbc8d6#.vm02lbsnw [https://perma.cc/S934-PVCA] (detailing female writer's personal experiences with online harassment).

17. *See infra* Section II.D (discussing legal roadblocks to effectively handling cyber harassment complaints).

18. *See infra* Section II.E (evaluating effectiveness of proposed doxxing and swatting legislation).

19. *See infra* Part III (examining free speech implications of doxxing and swatting and possible solutions).

20. *See* Recupero, *supra* note 6, at 325 (defining doxxing); Noah Berlatsky, *Doxing Isn't About Privacy—It's About Abuse*, DAILY DOT (Apr. 27, 2016), http://www.dailydot.com/via/doxing-privacy-abuse-online/ [https://perma.cc/F9AP-C4X9] (suggesting doxxing encompasses release of both public and private personal information); *see also* Megan Garber, *Doxing: An Etymology*, ATLANTIC (Mar. 6, 2014), http://www.theatlantic.com/technology/archive/2014/03/doxing-an-etymology/284283/ [https://perma.cc/2CB

scheme whereby they exploit basic information available through cursory Internet searching in order to capture victims' sensitive data such as passwords and Social Security Numbers (SSNs).[21] Although doxxing originated as a method for hackers to shame their online rivals, it has evolved into an aggressive form of cyber harassment.[22] Doxxers now routinely release a person's private information online with the intention of inciting other Internet users to harass that victim.[23] Widespread Internet use and accessibility allows geographically distant harassers to virtually "aggregate their efforts" against particular individuals, amplifying the abuse that victims experience.[24] Furthermore, the anonymity of the Internet emboldens harassers by allowing them to avoid social repercussions for their actions.[25]

Harassers aim to make victims feel vulnerable in real life by exposing their targets' information online.[26] For example, doxxers post their victims' home

U-Y5V5] (noting term "dox" originated from word "document"); Alex Goldman, *The Problem With "Doxxing"*, WNYC (Mar. 10, 2014), http://www.wnyc.org/story/problem-doxxing/ [https://perma.cc/V2CC-85SH] (highlighting older phrase "dropping dox," meaning "dropping documents" to describe doxxing).

21. *See* Recupero, *supra* note 6, at 325 (describing breadth of information released through doxxing); Jason Fagone, *The Serial Swatter*, N.Y. TIMES MAG. (Nov. 24, 2015), http://www.nytimes.com/2015/11/29/magazine/the-serial-swatter.html?_r=0 (explaining teen's piecemeal method of obtaining female gamers' information from online vendors and service providers); Sameer Hinduja, *Doxing and Cyberbullying*, CYBERBULLYING RES. CTR. (Sept. 16, 2015), http://cyberbullying.org/doxing-and-cyberbullying [https://perma.cc/4ZGN-SPC5] (suggesting most people unknowingly "seed" Internet with personal information).

22. *See* Citron, *Cyber Civil Rights*, *supra* note 7, at 69, 72-73, 75-80 (demonstrating ability to antagonize victims through doxxing); Berlatsky, *supra* note 20 (emphasizing link between doxxing and intimidation); Goldman, *supra* note 20 (detailing previous use of doxxing to shame other Internet users).

23. *See* Citron, *Cyber Civil Rights*, *supra* note 7, at 64-65, 80-81, 84 (highlighting purposely harmful exposure of private information online and criticizing mob mentality of online groups). Citron suggests that negative online posts serve as "calls to action" to other Internet users. *See id.* at 84; *see also* Berlatsky, *supra* note 20 (calling doxxing "weaponized attention"). Sociologist Katherine Cross suggests that doxxing "aggregat[es] specific data from [the] sea of data points" on the Internet and directs that information to "a hostile audience predisposed to hate the person in question." *See* Berlatsky, *supra* note 20.

24. Citron, *Cyber Civil Rights*, *supra* note 7, at 63-64 (suggesting Internet lets multiple harassers join forces against victims despite physical distance); Michael Barrett Zimmerman, Note, *One-Off & Off-Hand: Developing an Appropriate Course of Liability in Threatening Online Mass Communication Events*, 32 CARDOZO ARTS & ENT. L.J. 1027, 1044 (2014) (suggesting individually innocuous messages "engender[] . . . fear of violence" when aggregated); Joel Stein, *How Trolls Are Ruining the Internet*, TIME (Aug. 18, 2016), http://time.com/4457110/internet-trolls/ [https://perma.cc/6YU8-RJZ9] (recalling how 300,000 white supremacists joined forces on Twitter to harass actress Leslie Jones).

25. *See* Citron, *Cyber Civil Rights*, *supra* note 7, at 83 (suggesting web anonymity allows harassers to evade personal responsibility for tormenting victims). Citron posits that Internet mobs tend to affirm the dehumanization of harassment victims. *See id.* at 82; *see also* Becky Gardiner et al., *The Dark Side of Guardian Comments*, GUARDIAN (Apr. 12, 2016), https://www.theguardian.com/technology/2016/apr/12/the-dark-side-of-guardian-comments [https://perma.cc/56CM-ND6L] (suggesting "[a]nonymity disinhibits" Internet users, leading to "pil[ing] in" of other abusers).

26. *See* Citron, *Cyber Civil Rights*, *supra* note 7, at 69-71 (outlining real-world implications of revealing victims' personal information online); Berlatsky, *supra* note 20 (suggesting doxxing constitutes "violent act" of intimidation against victim); Peter Holley, *A Professor Called Trump's Election an 'Act of Terrorism.' Then She Became the Victim of Terror*, WASH. POST (Dec. 28, 2016), https://www.washingtonpost.com/news/grade-point/wp/2016/12/27/a-professor-called-trumps-election-an-act-of-terrorism-then-she-became-the-victim-of-ter

addresses, phone numbers, and photos along with encouragements to physically or sexually assault them.[27] Other doxxers put their victims in danger of identity theft by releasing their victims' SSNs and account passwords online.[28]

Following such incidents, many victims either stop or limit their public activity, both online and offline, out of fear of continued or worsened harassment.[29] In a world where the majority of adult Americans use the Internet, and where employees in dynamic fields such as journalism and technology are expected to have heavy online presences, this fear severely limits victims' opportunities for professional growth.[30] Victims who work primarily online are cut off from their professional networks and forced to seek alternative employment.[31] Even victims who do not work online are often forced to take time away from work to address harassment and its emotional and psychological consequences.[32] Moreover, because doxxed data remains

ror/?utm_term=.aa3d5ac69cf7 [https://perma.cc/QXW2-KG6D] (detailing professor's fear of physical violence after student posted video of professor criticizing Donald Trump).

27. *See* Citron, *Cyber Civil Rights*, *supra* note 7, at 70-71 (describing physical and sexual threats against doxxing victims). The hacker group Anonymous released a journalist's email and home addresses, and urged its members to "choke" her. *See id.* at 77. Similarly, users of the website Juicy Campus released a woman's cell phone number and dorm address and specified that she was "available for sex." *See id.*; *see also* Citron, *Expressive Value*, *supra* note 10, at 383 (highlighting violent threat made against chat room user's young daughter). Hackers posted a photo of one victim's young daughter online, along with the victim's home address and a suggestion to rape the victim's daughter. *See* Citron, *Expressive Value*, *supra* note 10, at 383.

28. *See* Citron, *Cyber Civil Rights*, *supra* note 7, at 70, 80, 103 (noting potential dangers of releasing victims' financial information online); Fagone, *supra* note 21 (suggesting doxxing increases risk for credit card fraud).

29. *See* Citron, *Expressive Value*, *supra* note 10, at 384-88 (discussing how cyber victims withdraw from public and online interaction for fear of physical harm); Joseph Russomanno, *Facebook Threats: The Missed Opportunities of* Elonis v. United States, 21 COMM. L. & POL'Y 1, 28 (2016) (stressing manner in which online threats alter victims' behaviors); Heidi Stevens, *Here's Hoping Lindy West's Dumping of Twitter Sets the Tone for 2017*, CHI. TRIBUNE (Jan. 4, 2017), http://www.chicagotribune.com/lifestyles/stevens/ct-lindy-west-leaves-twitter-balancing-0104-20170104-column.html (noting journalist's departure from Twitter after receiving rape threats directed at young daughter); *see also* Valenti, *supra* note 12 (positing online rape threats "make women want to lay low"). Valenti describes how one female software programmer feared leaving her property after experiencing death and rape threats online. *See* Valenti, *supra* note 12.

30. *See* Citron, *Expressive Value*, *supra* note 10, at 386-88 (suggesting online harassment can curtail victims' success in evolving fields including journalism and technology); Lipton, *supra* note 15, at 1112-13 (observing cyber victims who reduce online presence lose "personal and professional opportunities"); *see also* Andrew Perrin & Maeve Duggan, *Americans' Internet Access: 2000-2015*, PEW RES. CTR. (June 26, 2015), http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/ [https://perma.cc/3TLU-4HNF] (documenting study showing 84% of Americans used Internet in 2015); Aaron Smith, *Searching for Work in the Digital Era*, PEW RES. CTR. (Nov. 19, 2015), http://www.pewinternet.org/2015/11/19/searching-for-work-in-the-digital-era/ [https://perma.cc/VT6S-4YMW] (summarizing study finding 35% of Americans use social media platforms to research jobs).

31. *See* WEST, *supra* note 1, at 109 (asserting harassment depletes victims' time and financial resources); Citron, *Expressive Value*, *supra* note 10, at 376, 385-86 (arguing online harassment impedes victims' professional opportunities); Valenti, *supra* note 12 (highlighting damage to female bloggers' professional reputations after online harassment).

32. *See* WEST, *supra* note 1, at 109 (maintaining harassment completely consumes victims' time); Hess, *supra* note 16 (suggesting harassment costs women money in "legal fees, online protection services, and missed wages"). Writer Jessica Valenti emphasizes that online harassment costs victims time and money and explains

online until the harasser or the hosting site removes it, the information continues to corrode victims' professional and social reputations long after the initial harassment occurs.[33]

### *B. Overview of Swatting*

Swatting—or baiting Special Weapons and Tactics (SWAT) units to victims' homes under false pretenses—is the most extreme outcome of doxxing.[34] Typically, swatters use doxxed information to determine victims' locations and falsely report emergencies at the victims' homes to the local police, who then dispatch SWAT teams to those locations.[35] Like doxxers, swatters are motivated by personal animus towards their victims and aim to terrorize them by physically intruding into their private residences.[36] Swatting is extremely dangerous for both SWAT teams and victims, given both parties' misconceptions about the situation.[37] Moreover, a single unnecessary SWAT team execution diverts substantial police time and resources away from actual emergencies and wastes thousands of taxpayer dollars.[38]

that she limited public promotion of her work, hired security personnel, and paid for an online service to "scrub" her private information from the Internet after repeated online threats. *See* Hess, *supra* note 16 (describing Valenti's experience).

33. *See* Ann Bartow, *Internet Defamation as Profit Center: The Monetization of Online Harassment*, 32 HARV. J.L. & GENDER 383, 386-87 (2009) (highlighting how harassers seek to repeatedly link negative information to victims' names online); Citron, *Cyber Civil Rights*, *supra* note 7, at 73-74 (describing harassers' efforts to taint law students' reputation with professors and potential employers); Lipton, *supra* note 15, at 1112-13 (discussing permanence and accessibility of online harassment); Roese, *supra* note 10, at 123-24 (stressing permanence of reputational damage created by online harassment); Berlatsky, *supra* note 20 (suggesting repeatedly doxxing same information creates new harm).

34. *See* Recupero, *supra* note 6, at 325 (defining swatting).

35. *See* Enzweiler, *supra* note 15, at 2002-03 (outlining swatting process); McIntyre, *supra* note 6, at 115 (suggesting doxxing can allow swatters to locate victims); Fagone, *supra* note 21 (relaying how serial swatter progressed from doxxing to swatting victims); Anneliese Mahoney, *Doxxing and Swatting: New Frontiers in Online Harassment*, LAW STREET (May 8, 2017), https://lawstreetmedia.com/issues/technology/doxxing-swatting-online-harassment/ [https://perma.cc/776G-XJUR] (noting connection between doxxing and swatting).

36. *See* Enzweiler, *supra* note 15, at 2008-09 (suggesting swatting constitutes terrorism against social or political opponents); Recupero, *supra* note 6, at 325 (contending swatters intentionally target trauma survivors to re-inflict emotional pain); Fagone, *supra* note 21 (describing terror of being swatted). One victim described "open[ing] the door to the sight of rifles pointed at [her] from every direction." *See* Fagone, *supra* note 21.

37. *See* Jaffe, *supra* note 11, at 457 (highlighting shooting of swatting victim with rubber bullet after victim refused to cooperate with police); Enzweiler, *supra* note 15, at 2002 (recognizing "high degree of danger" for police and victims in swatting situations); Alexander, *supra* note 11 (suggesting police often inadvertently endanger swatting victims when responding to perceived emergencies); Fagone, *supra* note 21 (hypothesizing swatting victims mistake SWAT team for intruders and respond with violence).

38. *See* Jaffe, *supra* note 11, at 473 (explaining swatting constricts police resources, especially in small towns); Enzweiler, *supra* note 15, at 2007 (suggesting unnecessary SWAT deployments lead to ineffective policing and wasted financial resources). The wasted training and execution involved in a false SWAT raid can cost a police department up to $10,000. *See* Enzweiler, *supra* note 15, at 2007.

### *C. Gender- and Race-Based Nature of Doxxing and Swatting*

Online harassers disproportionately target women and people of color, worsening the physical and psychological effects of doxxing and swatting.[39] Online harassers routinely objectify women based on their physical appearances, and doxxing is regularly accompanied by threats of sexual violence.[40] Similarly, people of color are deluged with racially-derogatory harassment online, including frequent references to lynching and slavery.[41] Women of color often face particularly heinous harassment because they are targeted on account of both their race and gender.[42] Actress Leslie Jones

39. *See* Citron, *Cyber Civil Rights*, *supra* note 7, at 65-66 (noting online mobs "overwhelmingly target . . . traditionally subordinated groups" including women and people of color); Russomanno, *supra* note 29, at 32 (recognizing women more likely targets for online threats); McIntyre, *supra* note 6, at 116-17 (highlighting prevalence of online harassment against women); Maeve Duggan, *Online Harassment: Summary of Findings*, PEW RES. CTR. (Oct. 22, 2014), http://www.pewinternet.org/2014/10/22/online-harassment/ [https://perma.cc/5NXG-G4BZ] (surveying approximately 3,000 Internet users and finding women ages eighteen to twenty-four harassed most frequently); Gardiner et al., *supra* note 25 (demonstrating disproportionate abuse against website's female and minority writers). One online newspaper reviewed over seventy million comments on its site and found that the ten regularly-featured writers who received the most abuse were all either women, people of color, or both. *See* Gardiner et al., *supra* note 25*; see also* Kevin Munger, *Tweetment Effects on the Tweeted: Experimentally Reducing Racist Harassment*, 39 POL. BEHAV. 629, 630 (2017) (noting frequent harassment of people of color on social media). *But see* WORKING TO HALT ONLINE ABUSE, 2013 CYBERSTALKING STATISTICS 1 (2013), http://www.haltabuse.org/resources/stats/2013Statistics.pdf [https://perma.cc/Z34M-7TGA] (noting 60% of 256 harassment reports to organization came from women, with 78% caucasian respondents).

40. *See* WEST, *supra* note 1, at 113-14 (recalling personal online attacks leveled against author based on her weight); Citron, *Cyber Civil Rights*, *supra* note 7, at 64-65, 72, 75-76 (citing several examples of doxxing paired with threats of brutal gang rape); Citron, *Expressive Value*, *supra* note 10, at 383-84 (discussing online rape threats against several female victims); Hess, *supra* note 16 (highlighting rape and decapitation threat to female author); Sandra Laville et al., *The Women Abandoned to Their Online Abusers*, GUARDIAN (Apr. 11, 2016), https://www.theguardian.com/technology/2016/apr/11/women-online-abuse-threat-racist [https://perma.cc/YVR3-YGCS] (mentioning threat to rape female blogger "with wooden poles"); Valenti, *supra* note 12 (describing severe sexual harassment against author herself); Amy Wallace, *Life as a Female Journalist: Hot or Not?*, N.Y. TIMES (Jan. 19, 2014), http://www.nytimes.com/2014/01/20/opinion/life-as-a-female-journalist-hot-or-not.html (noting prevalence of attacks on female journalists' appearances); *see also* Bartow, *supra* note 33, at 392, 397 (illuminating disparate criticisms aimed at male and female writers). Bartow posits that "[e]ven when men are being insulted, the derogatory terms employed will often be references to female body parts." Bartow, *supra* note 33, at 397.

41. *See* Munger, *supra* note 39, at 631-32 (addressing rampant racism on social media); Alexander, *supra* note 11 (noting black female reporter received letters referencing "lynchings" and "a race war"); Gardiner et al., *supra* note 25 (revealing people of color constituted majority of most abused writers on site); Laville et al., *supra* note 40 (detailing images of "Ku Klux Klan cross burnings" posted to Black Lives Matter Facebook page); Terrell Jermaine Starr, *The Unbelievable Harassment Black Women Face Daily on Twitter*, ALTERNET (Sept. 16, 2014), http://www.alternet.org/unbelievable-harassment-black-women-face-daily-twitter [https://perma.cc/9MVS-ETS3] (describing lynching threats received by black actress). A study by the University of Michigan, which surveyed 340 African American, Latino, Asian, and biracial students, found that 64% of those students experienced at least one instance of racial discrimination online. *See* Brendesha Tynes, *Online Racial Discrimination: A Growing Problem for Adolescents*, AM. PSYCHOLOGICAL ASS'N. (Dec. 2015), http://www.apa.org/science/about/psa/2015/12/online-racial-discrimination.aspx (describing results of study about online discrimination against adolescents).

42. *See* Shireen Ahmed, *#MoreThanMean Video Highlights Daily Harassment Women in Sports Endure*, GUARDIAN (Apr. 28, 2016), https://www.theguardian.com/sport/2016/apr/28/more-than-mean-video-online-

became a prominent example of this two-pronged harassment after hackers infiltrated her website, doxxed her private information and photos, and incited a cyber-attack against her on Twitter.[43] The harassment ultimately forced Jones to temporarily leave the social networking site after it failed to respond to a barrage of racist and sexist tweets.[44]

Online harassment can be especially intense for victims who work in industries that are traditionally dominated by white men.[45] Feminist writers, as well as female sports reporters, gamers, and political activists have all been subjected to vitriolic online abuse centered on the victim's gender, race, or both.[46] This harassment not only dissuades women and people of color from participating in these fields, but also stifles opportunities for diverse perspectives in these industries.[47]

harassment-women-in-sports [http://perma.cc/U9FK-AN9H] (noting harassment directed towards Muslim female author "often steeped in racism"); Laville et al., *supra* note 40 (suggesting comments on Black Lives Matter Facebook pages contain "racism, sexism[,] and homophobia"); Lisa O'Carroll, *Gina Miller: 'I've Been Told That "as a Coloured Woman", I'm Not Even Human'*, GUARDIAN (Jan. 25, 2017), https://www.theguardian.com/politics/2017/jan/25/parliament-alone-is-sovereign-gina-miller-speaks-out-after-article-50-victory [https://perma.cc/8F5D-2ZG2] (highlighting racist threats against black female political activist in United Kingdom); Abby Ohlheiser, *The Leslie Jones Hack Used All the Scariest Tactics of Internet Warfare at Once*, WASH. POST (Aug. 26, 2016), https://www.washingtonpost.com/news/the-intersect/wp/2016/08/26/the-leslie-jones-hack-used-all-the-scariest-tactics-of-internet-warfare-at-once/ [https://perma.cc/48AF-4WY7] (suggesting women of color subjected to both racism and sexism online); Jaya Saxena, *The Abuse Leslie Jones Endured on Twitter Is Nothing New for Black Women*, DAILY DOT (Jul. 19, 2016), http://www.dailydot.com/irl/leslie-jones-twitter-abuse/ [https://perma.cc/2LFX-8LJA] (criticizing Twitter's apathetic reaction to online abuse against women of color). Writer Morgan Jerkins argues that Twitter is more responsive to abuse reports from white women than women of color. *See* Saxena, *supra*. For example, YouTube personality Akilah Hughes compares Twitter's immediate response to white singer Taylor Swift's harassment on the site to the company's lackadaisical response to the Leslie Jones attack. *See id*.

43. *See* Ohlheiser, *supra* note 42 (describing attack on Jones); Stein, *supra* note 24 (noting Jones received both "racist and sexist threats" online).

44. *See* Ohlheiser, *supra* note 42 (discussing aftermath of Jones attack); Saxena, *supra* note 42 (suggesting Twitter responded inadequately to Jones attack).

45. *See* Bartow, *supra* note 33, at 396 (linking violation of gender roles to increased online harassment). Bartow suggests that harassers view women who express "confident opinions on male-identified topics" as "unwomanly," and consequently feel justified in attacking those victims. *Id.*; *see* Russomanno, *supra* note 29, at 33 (positing harassers exploit power of online threats); Ahmed, *supra* note 42 (discussing harassment endured by female Muslim sports writer); Capelouto, *supra* note 13 (noting harassment of female gamers); Gardiner et al., *supra* note 25 (emphasizing number of abusive comments aimed at female writers covering "male-dominated" topics).

46. *See* Jenna Johnson, *This Is What Happens When Donald Trump Attacks a Private Citizen on Twitter*, WASH. POST (Dec. 8, 2016), https://www.washingtonpost.com/politics/this-is-what-happens-when-donald-trump-attacks-a-private-citizen-on-twitter/2016/12/08/a1380ece-bd62-11e6-91ee1adddfe36cbe_story.html?utm_term=.f47c914e5563 [https://perma.cc/3PXX-7TWT] (noting Trump attacked young woman on Twitter after she criticized his stance on women); O'Carroll, *supra* note 42 (describing racist threats made against black businesswoman who initiated anti-Brexit lawsuit); *supra* note 45 and accompanying text (describing online harassment of women in white, male-dominated fields).

47. *See* Citron, *Expressive Value*, *supra* note 10, at 391 (discussing how gendered online harassment silences female perspectives online); Russomanno, *supra* note 29, at 33 (suggesting online threats suppress victims' free speech); Shlomit Yanisky-Ravid & Amy Mittelman, *Gender Biases in Cyberspace: A Two-Stage Model, the New Arena of Wikipedia and Other Websites*, 26 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 381, 397-403 (2016) (arguing discrimination towards female Wikipedia editors shapes content available on site).

### *D. Barriers to Stopping Doxxing and Swatting*

#### *1. Lack of Accountability*

Despite the seriousness of both doxxing and swatting, harassers rarely face legal consequences for their actions.[48] Harassers can post destructive content anonymously, and often evade law enforcement officials by exploiting location-obscuring technology and jurisdictional boundaries.[49] Moreover, even if police can locate harassers, there are currently no federal statutes that specifically criminalize doxxing and swatting.[50] As a result, many doxxers and swatters are able to claim that their conduct is lawful, and that they are merely exercising their First Amendment right to free speech.[51] For example, in *Elonis v. United States*,[52] the Supreme Court further enabled perpetrators of doxxing and swatting when it suggested that online harassment only qualifies as a "true threat," or loses First Amendment protection, if harassers subjectively view their actions as threatening.[53] Under this standard, the

Michelle Ferrier, a former reporter and current associate dean at Ohio University, suggests that online harassment has a "chilling effect" on media participation by women and people of color. *See* Alexander, *supra* note 11 (noting Ferrier left her reporter position after receiving racist, violent threats). The lack of diversity among executives in many white-male-dominated industries exacerbates this issue because those executives often underestimate the need for antiharassment measures. *See* Laville et al., *supra* note 40 (criticizing tech industry executives for failing to prioritize antiharassment efforts on behalf of marginalized groups).

48. *See* Jaffe, *supra* note 11, at 467 (noting lack of federal laws addressing swatting); McIntyre, *supra* note 6, at 119-23 (elucidating issues with prosecuting doxxing cases); Capelouto, *supra* note 13 (suggesting anonymity of web shields online harassers from prosecution); Friedman, *supra* note 2 (highlighting "loophole[s]" in federal laws surrounding swatting).

49. *See* Citron, *Cyber Civil Rights*, *supra* note 7, at 83 (discussing online harassers' use of pseudonyms); Enzweiler, *supra* note 15, at 2002 (describing "spoofing" technology which hides swatters' phone numbers); Capelouto, *supra* note 13 (noting harassers attack victims anonymously using aliases and fake social media accounts). Although police knew the identity of a Canadian teenage serial swatter who attacked women throughout the United States, they were unable to arrest him for nearly a year due to state jurisdiction and minor extradition issues. *See* Fagone, *supra* note 21 (describing how serial swatter evaded police for months by targeting victims in different locations). This lag in prosecution emboldened the swatter, who posted about being "untouchable" and "unextraditeable." *See id.*

50. *See* Jaffe, *supra* note 11, at 479 (noting difficulty in proving "true threat" from online harassment after Supreme Court decision); McIntyre, *supra* note 6, at 119-22 (highlighting difficulty of prosecuting doxxing under existing criminal law); Fagone, *supra* note 21 (illustrating jurisdictional difficulties of swatting prosecution); Friedman, *supra* note 2 (discussing how no laws address false emergency reports unrelated to bombing or terrorism).

51. *See* U.S. CONST. amend. I (forbidding government infringement on freedom of speech); Elonis v. United States, 135 S. Ct. 2001, 2005-07, 2012-13 (2015) (sidestepping denunciation of Facebook threats as unprotected speech by avoiding free speech analysis altogether); United States v. Ossinger, 753 F.3d 939, 941, 943-44 (9th Cir. 2014) (discussing defendant's First Amendment protection claim for online publication of ex-girlfriend's nude photos); Doe I v. Individuals, 561 F. Supp. 2d 249, 253-54 (D. Conn. 2008) (suggesting doxxer in AutoAdmit case had First Amendment right to anonymous online speech). *But see* Citron, *Cyber Civil Rights*, *supra* note 7, at 106 (contending courts can successfully balance First Amendment and victims' rights).

52. 135 S. Ct. 2001 (2015).

53. *See id.* at 2011-12 (holding liability for harassment hinges on defendant's subjective understanding of harassment); Jaffe, *supra* note 11, at 477 (suggesting *Elonis* Court emphasized perpetrator's perception of

harassers have the ability to determine the severity of the harassment, making it much easier for defendants to evade prosecution.[54] Even more ludicrous, this decision allows harassers to impede victims' First Amendment rights under the guise of protecting the harassers' right to free speech.[55]

Accountability for doxxing and swatting is even further truncated by the Communications Decency Act (CDA), which shields Internet Service Providers (ISPs) from legal liability for the content that site users generate.[56] Originally, Congress created the CDA to shield ISPs that tried to remove offensive, user-generated content from their sites from further liability.[57] Nevertheless, federal courts greatly expanded the scope of the CDA through *Zeran v. America Online, Inc.*,[58] which insulated ISPs from liability for user-generated content even if aware of the antagonistic nature of the content.[59] The *Zeran* court reasoned that mandating removal of user-generated content would place an "impossible" commercial burden on ISPs.[60] Consequently, doxxing and

threats over victim's perception); Russomanno, *supra* note 29, at 32-33 (criticizing *Elonis* decision for refusing to label online harassment "low-value" unprotected speech). Conversely, in cases involving in-person, rather than online threats, the Court suggested that how victims perceive threats is relevant. *See* Virginia v. Black, 538 U.S. 343, 359-60, 363 (2003) (suggesting intimidation through cross-burning "true threat" due to perceptions of threat); Planned Parenthood of Columbia/Wilamette, Inc. v. Am. Coal. of Life Activists, 290 F.3d 1058, 1085-86 (9th Cir. 2002) (holding "wanted" posters of abortion providers constituted "true threat" by putting victims in fear).

54. *See Elonis*, 135 S. Ct. at 2016 (Alito, J., concurring in part and dissenting in part) (arguing context of online threat matters). Justice Alito suggests that online threats inflict damage regardless of harassers' intent, and contends that harassers should not be able to reframe their actions to attain constitutional protection. *See id.* Justice Alito also highlights domestic abusers' use of social media as a means of coercing their victims, and suggests that the Court should not protect such behavior. *See id.* at 2017; *see also* Jaffe, *supra* note 11, at 479-80 (highlighting ease of evading liability for online harassment after *Elonis*).

55. *See* Jennifer Elrod, *Expressive Activity, True Threats, and the First Amendment*, 36 CONN. L. REV. 541, 552-53 (2004) (contending threats suppress free speech); Russomanno, *supra* note 29, at 33-34 (arguing online harassment denies victims right to express their own ideas); *see also* Yanisky-Ravid & Mittelman, *supra* note 47, at 406-07 (2016) (criticizing courts for valuing online free speech over protection from cyber harassment).

56. *See* 47 U.S.C. § 230(c)(1) (2012) (limiting ISPs' liability for user-generated content). The CDA states that ISPs are not "treated as the publisher" of information posted by third-parties. *See id.*; *see also* Zeran v. Am. Online, Inc., 129 F.3d 327, 332 (4th Cir. 1997) (noting CDA prevents claims against ISPs for offensive content published by third-parties).

57. *See* Roese, *supra* note 10, at 130 (suggesting CDA originally intended to encourage ISPs "to remove offensive materials from their websites").

58. 129 F.3d 327 (4th Cir. 1997).

59. *See id.* at 332 (shielding ISPs from liability for user-generated content by labeling them publishers). The court reasoned that an ISP acting as a "publisher" by "publish[ing], edit[ing], or withdraw[ing]" online content would be immune from liability under the CDA. *See id.* at 332-33. Moreover, the court suggested that an ISP should not be liable for harmful content posted on its site, even if it was aware of the content, because forcing the ISP to remove all harmful content would place too great a burden on ISP operations. *See id.* at 333; *see also* Michal Lavi, *Content Providers' Secondary Liability: A Social Network Perspective*, 26 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 855, 869-70 (2016) (noting ISPs avoid liability even when aware of harmful content on their sites).

60. *See Zeran*, 129 F.3d at 333 (suggesting actively monitoring voluminous online posts unfairly burdens ISPs); *see also* Citron, *Cyber Civil Rights*, *supra* note 7, at 116 (theorizing courts extended ISPs' immunity

swatting victims cannot hold ISPs accountable for any harassment that occurs on their sites, and ISPs have very little incentive to remove abusive content.[61]

### *2. Lack of Understanding from Law Enforcement*

Law enforcement officers' misconceptions about online harassment often prevent victims' cases from being handled effectively.[62] Many law enforcement officers do not fully understand what doxxing and swatting entail, and do not have the technical knowledge or training needed to effectively respond to victims' complaints.[63] In addition, law enforcement officers often lack the time and the financial resources to pursue an effective investigation.[64] Many law enforcement officers also underestimate the gravity of doxxing and swatting, and as a consequence, react inappropriately to victims' reports.[65] Law enforcement agencies often respond dismissively to victims' complaints, advising victims to simply stop using the Internet, or telling victims that there is nothing that police can do to address the situation.[66] This indifference has

under CDA beyond legislators' original intent); Lipton, *supra* note 15, at 1132-33 (noting overbroad interpretation of CDA reduces redressability options for cyber harassment victims).

61. *See* Citron, *Cyber Civil Rights*, *supra* note 7, at 116 (arguing courts granted overbroad immunity under CDA); Lipton, *supra* note 15, at 1132-33 (emphasizing lack of liability under CDA disincentivizes ISPs from monitoring online content). AutoAdmit, a law school message board, and Juicy Campus, a college-themed gossip site, both refused to remove defamatory content posted about female students. *See* Roese, *supra* note 10, at 124-27 (noting AutoAdmit and Juicy Campus refused to remove abusive content). Similarly, WordPress.com reportedly told a doxxing victim who asked the site to remove photos of her children that their company was "in no position to arbitrate content disputes." *See* Laville et al., *supra* note 40 (recounting WordPress.com's dismissive response to victim's report of harassment through site).

62. *See* Citron, *Expressive Value*, *supra* note 10, at 402-03 (noting lack of police understanding of seriousness of cyberharassment); Alexander, *supra* note 11 (highlighting current weaknesses of police strategies for cyber harassment cases). Law enforcement agencies often do not understand the nature of online threats, or how to prevent them. *See* Alexander, *supra* note 11.

63. *See* Citron, *Expressive Value*, *supra* note 10, at 402-03 (underlining lack of cybercrime training for police); McIntyre, *supra* note 6, at 123 (suggesting police lagging in effective methods of combatting cyber harassment); Alexander, *supra* note 11 (stating most police lack technical skills necessary for protecting online information); Fagone, *supra* note 21 (highlighting difficulty of explaining swatting to untrained officer). One swatting victim compared explaining swatting to an untrained officer to explaining "drowning, [when] the person doesn't understand what water is." *See* Fagone, *supra* note 21.

64. *See* Fagone, *supra* note 21 (emphasizing 1,000 hours of individual officer's time spent pursuing teen swatter). One officer spent nearly a year tracking down a Canadian teen swatter and was forced to repeatedly collaborate with the Federal Bureau of Investigation (FBI), Canadian police, and various victims scattered across the country. *See* Fagone, *supra* note 21; *see also* Hess, *supra* note 16 (suggesting local police lack resources to investigate cyber-harassment while federal police lack incentive); Levintova, *supra* note 13 (detailing FBI's unwillingness to use financial resources on cybercrime training).

65. *See* Citron, *Expressive Value*, *supra* note 10, at 403 (suggesting police trivialize cyber harassment); Hess, *supra* note 16 (detailing inadequate response from FBI in relation to online harassment); Levintova, *supra* note 13 (suggesting police underestimate "real-life impact" of online threats).

66. *See* WEST, *supra* note 1, at 108-10 (describing FBI's apathy towards author's harassment complaint); Citron, *Expressive Value*, *supra* note 10, at 402-04 (underlining lack of police action against cyber harassment); Hess, *supra* note 16 (describing several women's frustration with underwhelming police response to cyber harassment). Many law-enforcement officials simply advise victims to "unplug" from the Internet. *See* Hess, *supra* note 16; *see also* Laville et al., *supra* note 40 (underlining police inaction after one victim made 126

severe consequences: it undermines victims' experiences and discourages future victims from coming forward.[67]

### *E. Proposed Legislation Surrounding Swatting and Doxxing*

Proposed legislation sponsored by Congresswoman Katherine Clark would help address the current lack of accountability and police action surrounding doxxing and swatting.[68] Congresswoman Clark's bills would target both the causes and effects of doxxing and swatting by deterring harassers, validate the seriousness of these actions, and expand cybercrime training opportunities for law enforcement agencies.[69]

Both the Interstate Swatting Hoax Act (Swatting Hoax Act) and the Interstate Doxxing Prevention Act (Doxxing Prevention Act) would deter harassers by criminalizing swatting and doxxing at the federal level.[70] Specifically, the Swatting Hoax Act would mandate that any person who intentionally "cause[s] an emergency response" from a law enforcement agency by falsely reporting a past, present, or future crime or public safety issue be subject to criminal penalties.[71] The proposed bill would account for the severity of a swatter's actions by providing for graduated criminal penalties depending on the ultimate harm that the swatting creates.[72] For example, a swatter who causes an emergency response alone could be fined, sentenced to up to five years in prison, or both.[73] Conversely, a swatter whose actions cause serious bodily injury could face up to twenty years in prison, while a swatter

reports about her harassment); Levintova, *supra* note 13 (noting lack of understanding of gravity of cyber harassment by police).

67. *See* Citron, *Expressive Value*, *supra* note 10, at 402 (noting cyber harassment underreported because victims fear police will not take their complaints seriously). Police minimize women's concerns about cyber harassment, making victims feel as though they need to either tolerate the harassment or go offline. *See id.* at 375-76.; *see also* Hess, *supra* note 14 (suggesting women made to feel reporting threats constitutes overreaction); Levintova, *supra* note 13 (discussing emotional toll of apathetic responses from law enforcement); *see also* Laville et al., *supra* note 40 (suggesting police inaction spurs online harassment victims to investigate harassers themselves).

68. *See* Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. § 2 (2016) (criminalizing doxxing); Cybercrime Enforcement Training Assistance Act of 2016, H.R. 4740, 114th Cong. § 2 (2016) (as referred to Subcomm. on Crim., Terrorism, Homeland Sec., and Investigations, Apr. 1, 2016) (allocating funding for police cybercrime training); Interstate Swatting Hoax Act, H.R. 4057, 114th Cong. § 2(a) (2015) (as referred to Subcomm. on Crim., Terrorism, Homeland Sec., and Investigations, Dec. 4, 2015) (criminalizing swatting).

69. *See supra* note 68 and accompanying text (creating framework for doxxing and swatting prevention).

70. *See* H.R. 6478, § 2 (criminalizing doxxing); H.R. 4057, § 2(a) (criminalizing swatting).

71. *See* H.R. 4057, § 2(a) (defining elements of swatting); Press Release, Congresswoman Katherine Clark, Clark Bill Aims to Combat Dangerous 'Swatting' Hoaxes (Nov. 18, 2015), http://katherineclark.house.gov/index.cfm/press-releases?ID=F71DAD9F-18E6-4B66-8B11-384911DE591B[https://perma.cc/3BCV-NF8Y] [hereinafter Press Release, Swatting] (describing bill's goal to update laws and "mak[e] it clear . . . 'swatting' is no joke").

72. *See* H.R. 4057, § 2(a) (specifying different repercussions for different levels of harm); Friedman, *supra* note 2 (noting bill punishes offenders based on amount of harm created).

73. *See* H.R. 4057, § 2(a) (listing graduated penalties for swatting).

who causes death could be imprisoned for life.[74] To offset the enormous financial costs of swatting, the Swatting Hoax Act would also require swatters to "reimburse any party" for expenses that the party incurred during unnecessary SWAT raids.[75]

Similarly, the Doxxing Prevention Act would penalize any individual who "knowingly publish[es]" another person's "personally identifiable information" in order to "threaten, intimidate, harass, [or] stalk" that person, or enable other individuals to do so.[76] Like the Swatting Hoax Act, the Doxxing Prevention Act would provide for a maximum five-year prison sentence and would create a civil cause of action for victims of doxxing.[77] The Doxxing Prevention Act would also acknowledge the wide-ranging consequences of doxxing by providing a broad definition of "personally identifiable information."[78] Under this bill, "personally identifiable information" would include both basic information such as the victim's name, date of birth, phone number, and address, as well as more sensitive information including the victim's SSN, "sexually explicit visual depiction[s]" of the victim, and the victim's demographic information.[79] Moreover, the Doxxing Prevention Act would create an objective standard by stipulating that the victim must "reasonabl[y] fear . . . death . . . or serious bodily injury" to herself, her immediate family member, or her partner.[80] By creating serious consequences for doxxing, the Doxxing Prevention Act seeks to protect victims and hold perpetrators legally accountable for their actions.[81]

In the same vein, the Cybercrime Enforcement Training Assistance Act of 2016 (Cybercrime Training Act) would facilitate more effective cybercrime prosecutions by issuing federal grants to expand cybercrime training at state and local levels.[82] State police departments, emergency dispatch workers,

74. *See id.* (describing penalties for swatting).

75. *See id.* § 2(c)(1) (mandating reimbursement for expenses incurred during SWAT team deployment).

76. *See* Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. § 2 (2016) (defining doxxing).

77. *See id.* (outlining penalties for doxxing).

78. *See id.* (creating broad definition for "personally identifiable information"). Under this bill, "personally identifiable information" is any information that can identify or be linked to a victim. *See id.*

79. *See id.* (giving examples of "personally identifiable information"). The Doxxing Prevention Act specifically mentions "gender identity" and "sexual orientation" as types of "personally identifiable information," but it is unclear whether information about race would be included in the general "biometric data" category listed in the bill. *See id.*

80. *See* H.R. 6478, § 2(a) (setting standard for doxxing prosecution).

81. *See* Press Release, Congresswoman Katherine Clark, Clark Bill Criminalizes Malicious Publication of Private Information (Dec. 8, 2016), http://katherineclark.house.gov/index.cfm/press-releases?ID=845879BE-5C95-4115-A5ED-A4BD79CA611B [https://perma.cc/92NJ-MWMM] [hereinafter Press Release, Doxxing] (explaining rationale for Doxxing Prevention Act). Congresswoman Clark has stated that doxxing victims "need to know that the law will protect them from criminals who jeopardize their safety," and contends that the Doxxing Prevention Act ensures that doxxing perpetrators "will be met by the full force of the law." *See id.*

82. *See* Cybercrime Enforcement Training Assistance Act of 2016, H.R. 4740, 114th Cong. § 2(a) (2016) (as referred to Subcomm. on Crim., Terrorism, Homeland Sec., and Investigations, Apr. 1, 2016) (allowing for federal grants to further cybercrime training).

prosecutors, and judges could use these grants to learn about state and federal resources for identifying, protecting, and assisting cybercrime victims, as well as how to use technology to investigate, prosecute, and adjudicate cybercrimes.[83] Moreover, state police could use the grants to create public cybercrime education programs and specialized cybercrime task forces, purchase updated technology, and cover the cost of expedited extradition requests for cybercrime perpetrators.[84] The Cybercrime Training Act aims to encourage information-sharing between law enforcement agencies and to provide officers with the cybercrime knowledge necessary to effectively assist victims.[85]

Together, all three of Congresswoman Clark's bills would help hold doxxing and swatting perpetrators accountable, validate the seriousness of these crimes, and expand the understanding of cybercrime on a state and national level.[86]

## III. ANALYSIS

Currently, there is no federal law in existence that sufficiently protects women and people of color from the real-life harms caused by doxxing and swatting.[87] Every day, doxxing and swatting victims are forced to endure a litany of financial, professional, psychological, and physical harm because courts, police, and legislatures refuse to acknowledge that online discrimination

83. *See id.* § 2(c) (outlining potential uses of grant money for cybercrime initiatives).

84. *See id.* (suggesting beneficial uses of cybercrime grants).

85. *See id.* § 2 (emphasizing cooperation between state and federal law enforcement agencies); Friedman, *supra* note 2 (discussing Congresswoman Clark's inspiration for Cybercrime Enforcement Training Assistance Act). Congresswoman Clark, who sponsored the bill, recognizes that "police officers want to help . . . [but] . . . just don't have training," and suggests that victims "need everybody to be able to know how to do a basic forensic investigation online." *See* Friedman, *supra* note 2; *see also* Press Release, Congresswoman Katherine Clark, Clark Cybercrime Training Proposal Gives Police Tools to Help Victims of Online Abuse (Mar. 16, 2016), http://katherineclark.house.gov/index.cfm/2016/3/clark-cybercrime-training-proposal-gives-police-tools-to-help-victims-of-online-abuse [https://perma.cc/5ANT-B9AT] [hereinafter Press Release, Training]. Clark hopes that the bill would allow law enforcement officers to help "victims regain their lives" following severe online harassment. *See* Press Release, Training, *supra*.

86. *See* Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. § 2 (2016); H.R. 4740, § 2; Interstate Swatting Hoax Act, H.R. 4057, 114th Cong. § 2(a) (2015) (as referred to Subcomm. on Crim., Terrorism, Homeland Sec., and Investigations, Dec. 4, 2015).

87. *See* Citron, *Cyber Civil Rights*, *supra* note 7, at 77, 80, 103 (explaining how online harassment compromises victims' physical and financial security); Citron, *Expressive Value*, *supra* note 10, at 383-84 (discussing gendered focus of online threats and violence); Russomanno, *supra* note 29, at 33-34 (arguing online harassment constrains victims' free speech rights); McIntyre, *supra* note 6, at 119-22 (discussing legal obstacles to doxxing and swatting prosecution); Press Release, Swatting, *supra* note 71 (stating falsely reporting emergencies not federal crime); Press Release, Doxxing, *supra* note 81 (emphasizing need for "clear cut federal prohibition" on doxxing); Ahmed, *supra* note 42 (noting women of color face both racism and misogyny online); *supra* notes 26-27 and accompanying text (arguing doxxing places victims at risk for physical and emotional harm); *supra* notes 37-38 and accompanying text (underlining danger and expense of swatting); *supra* Section II.C (discussing disproportionate targeting of women and people of color online).

and abuse often have severe offline consequences.[88] To the contrary, the legal system has emboldened harassers by allowing them to veil racist and misogynistic threats as "free speech," and failed victims by dismissing the harm that doxxing and swatting inflict.[89]

Nevertheless, the legislation proposed by Congresswoman Clark would provide the pivotal first steps in ensuring that online harassers are held to the same standard as their offline counterparts.[90] By holding doxxers and swatters accountable for their actions, validating the seriousness of victims' experiences, and equipping law enforcement agencies with the tools needed to combat online abuse, Congress can finally put an end to unchecked online harassment.[91]

### *A. Doxxing and Swatting as Racist and Misogynistic Methods of Intimidation*

Doxxers and swatters overwhelmingly target women, people of color, and most especially, women of color—specifically on account of their gender and race.[92] These harassers use language that focuses on their victims' physical

88. *See* Citron, *Cyber Civil Rights*, *supra* note 7, at 64 (emphasizing vicious online harassment of women and people of color); Citron, *Expressive Value*, *supra* note 10, at 403 (suggesting police trivialize cyber harassment); Jaffe, *supra* note 11, at 479 (arguing *Elonis* decision prevents prosecutors from proving "true threat" of online conduct); McIntyre, *supra* note 6, at 119-22 (outlining legal roadblocks to successfully prosecuting doxxing and swatting under existing law); *supra* notes 26-27 and accompanying text (outlining physical and emotional harm doxxing engenders); *supra* notes 37-38 and accompanying text (discussing danger and cost of swatting).

89. *See* Elonis v. United States, 135 S. Ct. 2001, 2016-17 (2015) (Alito, J., concurring in part and dissenting in part) (opining Court underestimated real-world harm of online threats); Citron, *Expressive Value*, *supra* note 10, at 402-03 (contending police trivialize cyber harassment); Jaffe, *supra* note 11, at 479-80 (arguing *Elonis* decision allows harassers to cloak threats as free speech); Russomanno, *supra* note 29, at 33-34 (criticizing *Elonis* decision for failing to protect online harassment victims' free speech rights); Yanisky-Ravid & Mittelman, *supra* note 47, at 406-07 (criticizing courts for prioritizing online free speech over victims' well-being); Levintova, *supra* note 13 (suggesting police unaware of "real-life impact" of online threats).

90. *See* H.R. 6478, § 2 (establishing criminal penalties for doxxing); H.R. 4740, § 2 (allocating federal funding for law enforcement cybercrime training); H.R. 4057, § 2(a) (criminalizing swatting at federal level); Jaffe, *supra* note 11, at 467 (highlighting current dearth of federal antiswatting statutes); Press Release, Swatting, *supra* note 71 (suggesting bill validates seriousness of swatting); Press Release, Doxxing, *supra* note 81 (stating bill would ensure apprehended doxxers face "full force of the law"); *supra* notes 48-50 and accompanying text (examining current lack of legal accountability for doxxing and swatting).

91. *See* Press Release, Swatting, *supra* note 71 (maintaining Swatting Hoax Act created to hold swatters accountable); Press Release, Doxxing, *supra* note 81 (affirming need to criminalize doxxing); Press Release, Training, *supra* note 85 (intending for Cybercrime Training Act to teach police how to aid victims more effectively); Friedman, *supra* note 2 (stating Cybercrime Training Act designed to train police on cybercrime prevention and investigation).

92. *See* Citron, *Cyber Civil Rights*, *supra* note 7, at 65-66 (noting disproportionate targeting of marginalized groups online); Ahmed, *supra* note 42 (addressing concurrently sexist and racist nature of comments aimed at Muslim female sports writer); Duggan, *supra* note 39 (indicating young women at highest risk for severe online harassment); Gardiner et al., *supra* note 25 (discussing disproportionate online harassment of newspaper's female and minority writers); Saxena, *supra* note 42 (highlighting racism and sexism women of color face online); Tynes, *supra* note 41 (describing study revealing frequent harassment of young people of color online); *supra* note 39 and accompanying text (relaying frequency and intensity of harassment against women and people of color); *supra* note 40 and accompanying text (highlighting gendered

appearances, and threaten gendered and racially charged violence.[93] Moreover, both doxxers and swatters intentionally target notable, vocal victims, often focusing on individuals who advocate for marginalized groups or who work in industries typically dominated by heterosexual, white men.[94] By visibly and viciously attacking these victims, doxxers and swatters hope to terrify them into silence and dissuade other diverse individuals from participating in future public discourse.[95] Doxxing and swatting surpass mere misogyny and racism by chilling victims' free speech, endangering their physical safety, and forcing them to withdraw from their communities.[96]

### *B. The Legal System's Enabling of Free Speech Suppression for Doxxing and Swatting Victims*

The legal system also enables the suppression of victims' First Amendment rights by minimizing the gravity of doxxing and swatting and allowing harassers to continue to infringe on victims' rights under the guise of "free speech."[97] Both the Court and law enforcement agencies demonstrate a gross misunderstanding of the real-world effects of doxxing and swatting, and seem willing to place blame for such harassment on the victims themselves.[98] Courts and police appear unwilling to evaluate online intimidation through the

nature of violent threats and harassment); *supra* note 42 and accompanying text (detailing two-pronged harassment of women of color online).

93. *See* Alexander, *supra* note 11 (examining race- and gender-based threats online); Laville et al., *supra* note 40 (discussing racially charged imagery used in online threats); *see also supra* note 40 and accompanying text (noting harassers focus on women's appearances and use gendered threats of violence); *supra* note 42 and accompanying text (describing racially charged and gendered threats against women of color).

94. *See* Johnson, *supra* note 46 (mentioning President Trump's harassment of woman who criticized his views on women); Levintova, *supra* note 13 (describing escalation of harassment against Congresswoman Clark after she began advocating against swatting); O'Carroll, *supra* note 42 (highlighting harassment of black female businesswoman who initiated anti-Brexit suit); *supra* notes 42-44 and accompanying text (recalling doxxing of actress Leslie Jones); *supra* note 45 and accompanying text (discussing harassment of women and people of color in traditionally white-male-dominated fields).

95. *See supra* note 29 and accompanying text (emphasizing many doxxing victims withdraw from public life); *supra* note 36 and accompanying text (calling swatting technique of intimidation); *supra* note 47 and accompanying text (arguing gender- and race-based harassment chills women and people of color's free speech).

96. *See supra* notes 26-33 (outlining real-world consequences of doxxing); *supra* note 37 (underlining physical danger of swatting); *supra* note 47 and accompanying text (evaluating free speech suppression created by online harassment).

97. *See* Elonis v. United States, 135 S. Ct. 2001, 2016 (2015) (Alito, J., concurring in part and dissenting in part) (noting ease with which harassers can exploit Court's subjective intent requirement in "true threat" cases); *supra* note 53 and accompanying text (exploring *Elonis* Court's reframing of restraints on threats to protect harassers' First Amendment rights); *supra* note 55 and accompanying text (suggesting online threats constrain real-world rights).

98. *See supra* notes 26-33 (discussing issues arising from doxxing); *supra* notes 37-38 (highlighting physical perils of swatting); *supra* notes 65-67 (describing law enforcement's dismissive attitude towards doxxing and swatting complaints); *see also Elonis*, 135 S. Ct. at 2016-17 (Alito, J., concurring in part and dissenting in part) (arguing Court needs to consider how online threats harm victims); Hess, *supra* note 16 (noting police advise women to "unplug" after online harassment).

same lens as purely in-person intimidation, even though both types of harassment are equally harmful.[99] Moreover, by allowing harassers to frame intimidation of women and people of color as "free speech," courts are inadvertently facilitating the derogation of these groups' First Amendment rights, leading to even greater marginalization.[100]

Because the legal system is not holding anyone accountable for harmful online content, victims have no way to advocate for their own rights.[101] Victims cannot rely on law enforcement agencies for protection, because those agencies lack the capacity to address victims' concerns appropriately.[102] Moreover, the anonymity of the web makes it difficult for victims to know who is attacking them, and the lack of legal repercussions for unmasked harassers has only emboldened doxxers and swatters.[103] Furthermore, ISPs have made it abundantly clear that they are unwilling to take down material that harms victims, eliminating yet another avenue of redress.[104] Given ISP and police unwillingness to help protect victims of online harassment, as well as the

99. *See Elonis*, 135 S. Ct. at 2016 (Alito, J., concurring in part and dissenting in part) (suggesting harm eminates from online intimidation regardless of harasser's intent); *supra* note 66 and accompanying text (illustrating several instances where police underestimated online harassment). The Court has been more likely to consider a victim's perception of threats in cases involving in-person, rather than online threats. *See* Virginia v. Black, 538 U.S. 343, 359-60, 363 (2003) (holding cross-burning constitutes "true threat" when used to intimidate); Planned Parenthood of Columbia/Willamette, Inc. v. Am. Coal. of Life Activists, 290 F.3d 1058, 1085-86 (9th Cir. 2002) (holding distribution of "wanted" posters for abortion providers constituted threat when used to intimidate).

100. *See* Citron, *Cyber Civil Rights*, *supra* note 7, at 106-11 (arguing online threats unprotected by First Amendment and suggesting legal avenues for victims); Russomanno, *supra* note 29, at 32-33 (contending *Elonis* Court erred by failing to deem online threats "low value" unprotected speech); *see also supra* note 47 and accompanying text (examining free speech deprivation created by gender- and race-based online harassment).

101. *See* Lipton, *supra* note 15, at 1132 (suggesting broad interpretation of CDA leaves cyber harassment victims with few options for redress); Friedman, *supra* note 2 (discussing "loophole[s]" in current cyber harassment statutes); *see also supra* note 48 and accompanying text (tracing lack of federal laws addressing doxxing and swatting); *supra* note 49 and accompanying text (highlighting issues with finding doxxers and swatters); *supra* note 58-60 and accompanying text (explaining how overbroad application of CDA eliminated ISPs' legal responsibilities for user content); *supra* note 61 and accompanying text (noting ISPs' disinterest in monitoring online content regardless of harm it inflicts).

102. *See* Friedman, *supra* note 2 (stating police want to help victims but lack adequate tools and knowledge to do so); Hess, *supra* note 16 (illuminating harassment victims' exasperation with lack of police response); Laville et al., *supra* note 40 (describing doxxing victims' attempts to alleviate harassment on their own after inappropriate police response); *see also supra* note 64 and accompanying text (stressing lack of police resources and training to investigate cybercrimes); *supra* note 66 and accompanying text (documenting current lack of legal response to doxxing and swatting).

103. *See* Citron, *Cyber Civil Rights*, *supra* note 7, at 83 (noting web anonymity shields cyber harassers from liability); Fagone, *supra* note 21 (recalling serial swatter calling himself "untouchable"); Levintova, *supra* note 13 (describing swatters audacious enough to attack current Congresswoman).

104. *See supra* note 61 and accompanying text (discussing ISPs' unwillingness to assist harassment victims).

disintegration of victims' free speech rights, it is unacceptable for the legislature to remain silent on this issue.[105]

### *C. How Proposed Legislation Could Help Protect Victims' Rights*

Congresswoman Clark's proposed legislation would remedy the lack of aid to marginalized victims of doxxing and swatting by forcing Congress to address harasser accountability, preventing race- and gender-based discrimination, and empowering law enforcement to combat online abuse.[106]

#### *1. Accountability*

Doxxers and swatters are evading responsibility for their actions primarily because there are no uniform federal laws specifically addressing this online conduct.[107] The Swatting Hoax Act and Doxxing Prevention Act would address this lack of accountability by criminalizing swatting and doxxing at the federal level.[108] Criminalizing doxxing and swatting would create a cohesive national policy on these types of harassment and ensure a uniform police response to victims' complaints regardless of where the harassment takes place.[109] Moreover, although locating harassers could still be problematic, the maximum criminal penalties under both bills—up to life in prison for swatting and up to five years in prison for doxxing—would ensure that the perpetrators who are caught face appropriate consequences.[110] Although the penalties under

105. *See* Citron, *Cyber Civil Rights*, *supra* note 7 at 83-84 (criticizing current lack of repercussions for online harassment); *supra* notes 29-33 and accompanying text (exploring how doxxing constrains victims' engagement with others); *supra* note 47 and accompanying text (suggesting online harassment stifles free speech); *supra* notes 56-61 (highlighting lack of ISP accountability); *supra* Section II.D.2 (detailing half-hearted responses by law enforcements agencies).

106. *See* Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. § 2 (2016) (criminalizing publication of personally identifiable information); Cybercrime Enforcement Training Assistance Act of 2016, H.R. 4740, 114th Cong. § 2 (2016) (as referred to Subcomm. on Crim., Terrorism, Homeland Sec., and Investigations, Apr. 1, 2016) (providing for police cybercrime training grants); Interstate Swatting Hoax Act, H.R. 4057, 114th Cong. § 2(a) (2015) (as referred to Subcomm. on Crim., Terrorism, Homeland Sec., and Investigations, Dec. 4, 2015) (criminalizing false emergency reports); *supra* notes 70-78 and accompanying text (describing how bills would create legal consequences for doxxing and swatting); *supra* note 79 and accompanying text (highlighting Doxxing Prevention Act's focus on gender); *supra* notes 82-85 and accompanying text (noting Cybercrime Training Act would allow for enhanced cybercrime education).

107. *See* Jaffe, *supra* note 11, at 467 (emphasizing gaps in federal laws in regard to swatting); McIntyre, *supra* note 6, at 119-23 (suggesting many current criminal remedies inadequately address doxxing); Friedman, *supra* note 2 (noting "loophole[s]" in federal laws surrounding cyber harassment).

108. *See* H.R. 6478, § 2 (making doxxing federal criminal offense); H.R. 4057, § 2(a) (creating federal criminal liability for swatting); Press Release, Swatting, *supra* note 71 (expressing desire to update federal statutes related to swatting).

109. *See* H.R. 6478, § 2 (calling for federal doxxing prosecution); H.R. 4057, § 2(a) (ensuring federal swatting prosecution); *see also* Fagone, *supra* note 21 (demonstrating inefficiency of prosecuting swatting cases without cohesive federal law); Hess, *supra* note 16 (suggesting federal law enforcement agencies currently lack incentive to pursue cyber harassment claims).

110. *See* H.R. 6478, § 2 (setting out maximum five-year prison sentence for doxxing); H.R. 4057, § 2(a) (providing maximum life prison sentence in event of swatting-related death); *see also* Citron, Cyber *Civil*

both bills would be significant, each bill would effectively signal to courts, law enforcement agencies, and harassers that prosecuting doxxing and swatting is a serious legal priority.[111] Finally, the broad definitions used for both doxxing and swatting under these bills would capture the wide range of conduct that victims can experience, thereby limiting a perpetrator's ability to argue that they did not violate the statutes.[112]

### *2. Addressing Race- and Gender-Based Motivations of Harassers*

Ensuring that both courts and law enforcement agencies appreciate the roles that racism and misogyny play in doxxing and swatting will be instrumental in combatting these types of online abuse.[113] In particular, the Doxxing Prevention Act would draw attention to the gendered nature of online harassment by specifically referencing gender identity, sexual orientation, and "sexually explicit depictions" as types of "personally identifiable information" protected by the statute.[114] Criminalizing the release of gender-related information acknowledges the disproportionality of online attacks against women and rightfully shifts responsibility for the release of such harmful information from victims to their aggressors.[115]

Nevertheless, the Doxxing Prevention Act falls short by failing to similarly highlight the racially motivated nature of doxxing.[116] The racism and misogyny that fuel doxxing and swatting are inextricably intertwined, and the legal protections created by this bill, especially for women of color, would be weakened if the final bill does not specifically address that reality.[117] Congress could easily address this issue by amending the Doxxing Prevention Act to

*Rights*, *supra* note 7, at 81-83 (underlining how anonymity of Internet contributes to online harassment and allows perpetrators to compartmentalize their actions); Enzweiler, *supra* note 15, at 2002 (noting swatters can often obscure their locations); Gardiner et al., *supra* note 25 (suggesting anonymity escalates volume of online abuse).

111. *See* H.R. 6478, § 2 (prioritizing doxxing prosecution); H.R. 4057, § 2(a) (mandating up-to-life sentence for death caused by swatting); Press Release, Doxxing, *supra* note 81 (describing intention to meet doxxing perpetrators with "full force of the law"); Press Release, Swatting, *supra* note 71 (suggesting Swatting Hoax Act meant to reaffirm seriousness of crime).

112. *See* H.R. 6478, § 2(a) (creating broad definition for "personally identifiable information"); H.R. 4057, § 2(a) (providing expansive definition of swatting); *supra* notes 29-33 (discussing real-world consequences of doxxing); *supra* notes 37-38 (describing danger and expense of doxxing and swatting); *supra* note 48 and accompanying text (outlining current issues with enforcement).

113. *See supra* Section II.C (exploring how gender and race motivate doxxers and swatters).

114. *See* H.R. 6478, § 2(a) (specifying "personally identifiable information" includes information related to gender and sexuality).

115. *See id.*; Citron, *Expressive Value*, *supra* note 10, at 397, 403-04 (highlighting frequent trivialization and victim-blaming of crime against women); Hess, *supra* note 16 (noting victim felt blamed for her harassment); Laville et al., *supra* note 40 (noting police faulted victim for responding to harasser); *supra* note 39 and accompanying text (covering harassers' disproportionate targeting of women and people of color).

116. *See* H.R. 6478, § 2 (mentioning "biometric data" but failing to explicitly highlight race-related doxxing issues).

117. *See supra* notes 41-42 and accompanying text (discussing frequency of race-based online harassment for women of color).

include race-specific language that mirrors the gender-specific provisions already included in the bill.[118]

Similarly, the Cybercrime Training Act would help expand the legal system's understanding of the causes and effects of doxxing and swatting.[119] This act would enable police, prosecutors, and judges to learn how to identify and assist cybercrime victims and would mandate participation in a national cybercrime database.[120] In doing so, the Cybercrime Training Act would both underscore the gravity of victims' experiences and bring the race- and gender-based natures of these crimes to the attention law enforcement, prosecutors, and the judiciary.[121] The more that police, prosecutors, and judges understand about the scope of doxxing and swatting, the more effectively they can help victims address the aftermath of these types of online abuse.[122]

### *3. Giving Law Enforcement Agencies the Right Tools to Combat Harassment*

Currently, law enforcement agencies do not have the appropriate tools or knowledge to effectively assist doxxing and swatting victims.[123] The policies promoted by the Cybercrime Training Act would give police the resources that they need to understand cybercrime and how to combat it.[124] The bill would streamline the doxxing and swatting investigation processes by giving officers access to the technology and training needed to investigate cybercrimes and by encouraging state and federal law enforcement agencies to share information.[125] With a better understanding of the nature of online harassment, and available tools to help fight it, law enforcement officers could become the first line of defense against threatening online behavior.[126] In turn, that network of legal support could help make victims feel more comfortable and confident coming to police after experiencing doxxing and swatting.[127]

118. *See* H.R. 6478, § 2 (including gender under "personally identifiable information").

119. *See* Cybercrime Enforcement Training Assistance Act of 2016, H.R. 4740, 114th Cong. § 2 (2016) (providing for enhanced cybercrime training for law enforcement officials).

120. *See id.* (describing scope of cybercrime program).

121. *See id.* (listing prerequisites for grant disbursement through cybercrime training program).

122. *See id.* (outlining increased cybercrime training opportunities for police, prosecutors, and judges); Press Release, Training, *supra* note 85 (suggesting bill intended to help police aid victims effectively).

123. *See supra* note 64 and accompanying text (discussing lack of police resources for combatting cybercrime).

124. *See* H.R. 4740, § 2 (allocating funds for cybercrime training and prevention); Friedman, *supra* note 2 (stating bill designed to teach officers about basic cybercrime investigations).

125. *See* H.R. 4740, § 2 (streamlining cybercrime investigations and encouraging intergovernmental cooperation); Press Release, Training, *supra* note 85 (explaining funds from bill would allow officers to learn effective cybercrime management and prevention).

126. *See* Press Release, Training, *supra* note 85 (expressing desire to empower officers to protect their communities); Friedman, *supra* note 2 (emphasizing officers' seeming interest in helping cybercrime victims).

127. *See* Citron, *Expressive Value*, *supra* note 10, at 402-03 (discussing police underestimation of cyber harassment and need for police involvement and training); Hess, *supra* note 16 (explaining lack of standardized police procedures for responding to online harassment); Levintova, *supra* note 13 (suggesting lackluster police responses to cyber harassment complaints exacerbate victims' trauma); *supra* note 66 and accompanying text

## IV. CONCLUSION

Doxxing and swatting may originate online, but they often lead to devastating consequences in real life. Doxxers and swatters use online harassment as a tool for chilling the speech of women and people of color and discouraging other diverse individuals from engaging in public discourse, both online and in the community. Unfortunately, the current lack of federal laws specifically addressing doxxing and swatting, along with police disinterest in pursuing doxxing and swatting claims, have left victims with few options for redress. In addition, the absence of legal accountability for doxxers and swatters, combined with the legal system's blasé attitude towards the financial, emotional, physical, and professional consequences of their actions, further marginalize disadvantaged societal groups.

The legislation proposed by Congresswoman Katherine Clark would alleviate the issues created by doxxing and swatting by validating the seriousness of such conduct, holding doxxers and swatters accountable for their harmful actions, and giving police access to the training and resources crucial to combatting online harassment. Although the bills would not completely eradicate online harassment, they represent an important first step in changing the public's perception of online abuse. Until Congress chooses to take action, victims, and their rights to free speech, will hang in the balance.

*Svana M. Calabro*

(discussing inadequate police response to cyber harassment); *see also* Press Release, Doxxing, *supra* note 81 (emphasizing importance of victims knowing "law will protect them from criminals who jeopardize their safety"); Press Release, Training, *supra* note 85 (suggesting Cybercrime Training Act would help victims "regain their lives").