St. Mary's Law Journal

Volume 52 | Number 3 Article 8

10-29-2021

The Dangers of Doxing and Swatting: Why Texas Should Criminalize These Malicious Forms of Cyberharassment

Hannah Mery
St. Mary's University School of Law

COMMENT

THE DANGERS OF DOXING AND SWATTING: WHY TEXAS SHOULD CRIMINALIZE THESE MALICIOUS FORMS OF CYBERHARASSMENT

HANNAH C. MERY*

* The author would like to thank her family and friends for their unceasing encouragement and support. She feels very blessed to have such a loving family and to have met such amazing people during her law school journey. Specifically, she would like to thank her parents, Bruce and Lori Mery, and her little brother, Aaron, for their constant love, patience, and much-needed hugs. Finally, the author would like to thank the Volume 52 Board and editing team for their hard work in editing this Comment.

I. INTRODUCTION

The #MeToo movement left an enormous impact on the legal world.[1] Intended to spark a "cultural transformation by 'encouraging millions to speak out about sexual violence and harassment,'" the movement became a "worldwide phenomenon, searched for on Google in 196 countries [in a year's time]."[2] The #MeToo movement also rocked the entertainment industry, especially in the wake of high-profile lawsuits like the Harvey Weinstein case.[3] Though the movement started a dialogue and helped

1. *See generally* Symposium, *Law & the #MeToo Movement*, STEIN SCHOLARS SYMP. (2019), https://www.fordham.edu/download/downloads/id/12642/me_too_cle_materials.pdf [https://perma.cc/HMU8-TRKF] (presenting a collection of materials for a CLE course covering "Law & the #MeToo Movement").

2. *See* Alix Langone, *#MeToo and Time's Up Founders Explain the Difference Between the 2 Movements—And How They're Alike*, TIME (Mar. 22, 2018, 5:21 PM), https://time.com/5189945/whats-the-difference-between-the-metoo-and-times-up-movements/ [https://perma.cc/KS8Q-Y668] (describing the #MeToo movement as well at the Time's Up movement, a similar movement focused on "creat[ing] concrete change, leading to safety and equity in the workplace").

3. *See* Daniel D'Addario, *What Happens to Hollywood Projects Tainted by Allegations of Sexual Misconduct?*, TIME (Dec. 21, 2017, 1:14 PM), https://time.com/5068752/hollywood-sexual-miscon

expose some of the corrupt systems perpetuating the proliferation of sexual harassment and violence,[4] some aspects of society and the entertainment industry remain separated from the #MeToo tide. Online abuse is one such area that has not gained this attention; this type of abuse many experience online "includes not only abusive comments and trolling, but also rape threats, death threats, and offline stalking."[5] Online abuse can also lead to psychological harms "as severe, and sometimes more severe, [than] harassment endured in the physical world."[6] A pertinent example of brutal, life-changing, and even deadly online abuse occurs in a part of the entertainment industry also removed from the #MeToo movement—the video game industry.[7]

For many, video games are an escape from everyday life.[8] Historically, games were simple and gender-neutral like Tetris, but with time, games became geared toward males due to marketing strategies targeting the majority-male audience.[9] Though women continued playing and still

duct-projects/ [https://perma.cc/B8UF-T5Z3] ("What started with the downfall of Harvey Weinstein became perhaps the most seismic shift the entertainment industry has ever undergone.").

4. Langone, *supra* note 2.

5. Jennifer Beckett & Monica Whitty, *#MeToo Must Also Tackle Online Abuse*, THE CONVERSATION (Mar. 21, 2018, 3:34 PM), https://theconversation.com/metoo-must-also-tackle-online-abuse-93000 [https://perma.cc/ZGG5-7RCK].

6. *See id.* (stating targets of offline harassment are also often the targets of online harassment and that online harassment may, in some instances, be more challenging for victims to cope with, as they may feel there is no escape).

7. *See Time for Harassers to Be Held Accountable, Female Gamer Says*, NPR (Jan. 9, 2018, 5:06 AM), https://www.npr.org/2018/01/09/576669374/time-for-harassers-to-be-held-accountable-female-gamer-says [https://perma.cc/DP6L-4P99] [hereinafter *Accountable*] (stating in an interview with Brianna Wu, a victim of a "campaign of harassment and abuse" called Gamergate, that Wu, and other women who advocated for greater inclusion for women in the video game field, "received . . . an extreme avalanche of death threats and rape threats and [experienced] the destruction of [their] personal lives in a way that was . . . horrifying for many people to watch").

8. *See* Noreen Malone, *Zoë and the Trolls: Video-Game Designer Zoë Quinn Survived Gamergate, an Act of Web Harassment with World-Altering Implications*, N.Y. MAG. (July 24, 2017), http://nymag.com/intelligencer/2017/07/zoe-quinn-surviving-gamergate.html [https://perma.cc/TEP9-R9N5] (discovering at a video game conference that "all anyone wanted . . . was to be able to imagine themselves in [those] imaginary worlds. A refuge from the more difficult one . . .").

9. *See id.* (outlining the video game industry's history and the gradual transformation of a gender-neutral industry into one dominated by and geared toward males).

constitute a sizable percentage of gamers,[10] stereotypes did, and continue to, perpetuate the thinking that gamers were solely male.[11]

II. DOXING, SWATTING, AND CYBERSTALKING—THE EXAMPLE OF GAMERGATE

Many women have stepped into the spotlight and challenged these stereotypes, but most have faced bullying, harassment, and personal threats.[12] These threats typically appear online through posts on social media or via email.[13] These online harassers, often called "trolls,"[14] may send death and rape threats, sometimes, rendered even more disturbing by stalking, "doxing" (also spelled "doxxing"), and "SWATing" (also spelled "swatting") their targets.[15] One particularly infamous series of coordinated,

10. Gaming statistics are hard to gather and break down. For this reason, statistics regarding the percentage of female players can be controversial in the "core gaming" community, which largely considers "real" gamers as those who play involved games on computers and consoles instead of casual games on smartphones. Thus, organizations such as the Entertainment Software Association (ESA) define gaming statistics differently than how real gamers would define them, combining statistics of players who play casual games on smartphones with statistics of real gamers who play more involved genres, such as action or adventure games. Nick Yee, *Beyond 50/50: Breaking Down the Percentage of Female Gamers by Genre*, QUANTIC FOUNDRY (Jan. 19, 2017), https://quanticfoundry.com/2017/01/19/female-gamers-by-genre/ [https://perma.cc/G65Q-ZHLL]. The ESA statistics, which include casual, smartphone gamers, said in 2019 that 46% of gamers were female while 54% were male. *2019 Essential Facts About the Computer and Video Game Industry*, ENT. SOFTWARE ASS'N 7 (2019), https://www.theesa.com/wp-content/uploads/2019/05/ESA_Essential_facts_2019_final.pdf [https://perma.cc/67FC-333A]. Females who are considered real gamers, however, constitute a smaller percentage than is listed in the ESA statistics. Yee, *supra* note 10.

11. *See* Dmitri Williams, Nick Yee, & Scott E. Caplan, *Who Plays, How Much, and Why? Debunking the Stereotypical Gamer Profile*, 13 J. COMPUTER-MEDIATED COMMC'N 993, 995 (2008) (stating movies and print media typically portray video game players as young and male).

12. *See, e.g.*, Helene Schumacher, *Harsh Realities of Being a Professional 'Girl Gamer'*, BBC, https://www.bbc.com/worklife/article/20180417-harsh-realities-of-being-a-professional-girl-gamer [https://perma.cc/37LM-9S5V] (relating the experiences of two female gamers, one of whom is a video game developer, participating in the industry and competing in professional gaming tournaments and the pushback they receive from male gamers, ranging from a lack of respect and belief in their skills as gamers to rape threats).

13. *See, e.g.*, Zachary Jason, *Game of Fear*, BOS. MAG. 2, 3 (Apr. 28, 2015, 5:45 AM), https://www.bostonmagazine.com/news/2015/04/28/gamergate/ [https://perma.cc/NG3U-5D5P] (explaining "social media amplifies the ability of online harassers to inflict damage on their victims" and describing how a woman who was attacked by online harassers received death threats by email).

14. *See Troll (Entry 3 of 3)*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/troll#h3 [https://perma.cc/UG88-9YNY] (defining a troll as "a person who intentionally antagonizes others online by posting inflammatory, irrelevant, or offensive comments or other disruptive content").

15. *See* Jim Edwards, *FBI's 'Gamergate' File Says Prosecutors Didn't Charge Men Who Sent Death Threats to Female Video Game Fan—Even When Suspects Confessed*, BUS. INSIDER (Feb. 16, 2017, 4:12 AM),

brutal attacks on female gamers became known as Gamergate.[16] Eron Gjoni, ex-boyfriend of video game developer, Zoë Quinn, ignited the Gamergate movement after the couple's breakup by crafting a demeaning post titled "The Zoe Post."[17] This post detailed their relationship and sparked a torrent of online attacks against Quinn.[18] Gjoni's conduct eventually led to the wide distribution of Quinn's personal information.[19] The post gained immense online attention, sparking the anger of men who believe women have no place in video games. Many of these men chose to attack Quinn and other women in the industry with graphic rape and death threats.[20]

Another woman targeted in Gamergate was Brianna Wu, a video game developer and founder of the game studio Giant Spacekat.[21] A determined entrepreneur, Wu was working to advance her company's popularity in the

https://www.businessinsider.com/gamergate-fbi-file-2017-2 [https://perma.cc/7T7N-MLCY] ("The women [who were harassed online] received dozens of scary late-night phone calls, threatening social-media posts, doxxing attempts, identity thefts, and . . . a successful 'swatting' hoax that sent five police officers to a home in Washington state to investigate a false report of a hostage situation."); *see also* Jason, *supra* note 13, at 3 (quoting Zoë Quinn's description of attackers as "stalking, sending death threats, trying to get the cops to raid homes").

Doxing is a slang term for "dropping documents" and "refers to gathering an individual's Personally Identifiable Information (PII), such as home address, telephone number and/or email address, and posting it publicly without permission." SWATing, as the name indicates, "is an internet prank/crime in which someone finds your address either through your computer's IP address, or because your name and location is known. They then anonymously call 911 and report a fake emergency." SWATing has resulted in death. TEX. DEP'T OF INFO. RES., OFF. OF THE CHIEF INFO. SEC. OFFICER, THE STATE OF TEXAS GUIDE TO DOXXING & SWATING 1–2 (2019), https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/OCISO%20Doxxing%20SWATing%202019.pdf [https://perma.cc/3LA4-K3FJ] [hereinafter TEXAS GUIDE].

16. Edwards, supra note 15; *see also* Jason, supra note 13 (describing Gamergate).

17. *The Zoe Post*, WORDPRESS (Aug. 16, 2014), https://thezoepost.wordpress.com/ [https://perma.cc/EV79-XZKV]; *see also* Joey L. Blanch & Wesley L. Hsu, *An Introduction to Violent Crime on the Internet*, U.S. ATT'YS' BULL., May 2016, at 3, 6 ("While [Quinn's ex-boyfriend] did not expressly threaten [her], his posting was filled with her personal information, and she contends that he was aware that his post would result in her being harassed and stalked by individuals reading the post. That is certainly what happened.").

18. *Id.*

19. *See* Jason, *supra* note 13 (presenting the statements Quinn made to the judge: "My personal info like my home address, phone number, emails, passwords, and those of my family has been widely distributed, alongside nude photos of me, and several of my professional accounts and those of my colleagues have been hacked.").

20. One such rape threat Quinn received stated: "[I'm] not only a pedophile, [I've] raped countless teens, this [Zoë] bitch is my next victim, [I'm] coming[,] slut." Another threat she received manifested when a harasser changed her Wikipedia biography to indicate she died during her next public appearance. *Id.* at 1, 3.

21. *Id.* at 3.

gaming industry when Gamergate took aim at her.[22] She had recently secured a spot on "Steam Greenlight, a powerful online distribution channel for new gamers" when she finally had enough of the abuse Gamergaters aimed at her friends and other women.[23] One night on her podcast, Wu stated:

> "You cannot have 30 years of portraying women as bimbos, sex objects, second bananas, cleavage-y eye candy . . . . Eventually it normalizes this treatment of women. And I think something is really sick and broken in our culture."[24]

The backlash was brutal, including graphic and disturbing threats.[25] Eventually Wu and her husband fled their home after doxing revealed her home address.[26] She even had to pull Giant Spacekat from the influential PAX East gaming conference after police declined to increase security despite the death threats she received over social media and email.[27]

Courts and law enforcement did not seem to—and often still do not—understand the implications of these attacks, with many dismissing evidence and downplaying the gravity of threats and harm the victims suffer, sometimes due to confusion regarding how the internet works.[28] Quinn speaks of one judge in particular who "suggested that [she] get a job that didn't involve the internet, if the internet had been so bad to her."[29] When she explained, "there was no offline version of what she did[,]" he replied, "You're a smart kid, ... Find a different career."[30] This, for Quinn, "was

22. David Whitford, *Brianna Wu vs. the Gamergate Troll Army*, INC. (Apr. 2015), https://www.inc.com/magazine/201504/david-whitford/gamergate-why-would-anyone-want-to-kill-brianna-wu.html [https://perma.cc/NV93-2A5D].

23. *Id.*

24. *Id.*

25. *Id.*

26. Wu states: "I laugh off 90 percent of the stuff I'm sent . . . [b]ut it's the 10 percent. If we don't change the culture, somebody's going to get killed." One particularly frightening threat Wu received revealed Wu's home address and stated: "Guess what bitch? I now know where you live [. . .] your mutilated corpse will be on the front page of Jezebel tomorrow . . . ." *Id.*

27. Jason, *supra* note 13, at 3; Whitford, *supra* note 22.

28. *See* Jason, *supra* note 13, at 3 ("Wu claims she los[t] at least a day each week 'explaining the Internet' to the police . . . [and] that she[] had to convince numerous officers that Twitter isn't 'just for jokes,' but is in fact her primary means of marketing her business."); *see also* Malone, *supra* note 8 ("When Quinn first reported the harassment to the police, they were confused, and wouldn't accept the USB drive she presented as evidence, so she printed the worst of the worst . . . .").

29. Malone, *supra* note 8.

30. *Id.*

one of the most coldhearted moments of the whole ordeal."[31] Not only does this statement speak to the ignorance many in the law have regarding the importance of the internet in today's society,[32] it also raises a problem many, not only women, experience in the workplace—the expectation that they roll with the punches and put up with harassment and disparaging comments or find a different job.[33]

On an NPR broadcast in 2018, Wu commented on the Gamergate crisis, which took place largely in 2014 and 2015.[34] She stated: "we are not having a #MeToo moment at all. I think what a lot of women in the game industry saw with Gamergate is they saw if they came forward, help was not going to come."[35]

III. CYBERHARASSMENT'S BROAD RAMIFICATIONS AND PROPOSAL FOR A SOLUTION

Cyberharassment, accomplished through attacks such as doxing and swatting, has led to nationwide ramifications affecting both citizens and the nation in general. These ramifications include the chilling of victims' speech, which, in turn, leads to societal and economic harm.[36] Though this

31. *Id.*

32. Many jobs and careers now consider a social media presence as simply an aspect of the job. For example, politicians and businesspeople often use social media to advertise their platforms or products. For that reason, many cannot simultaneously avoid the internet and adequately perform their jobs. *See* Beckett & Whitty, *supra* note 5 ("For women working in public-facing roles in politics, business, and the media (and even academia)—where social media use is often seen as 'part of the job'—the problem [of online abuse] is worse.").

33. When people join workplaces where they are different from most of their coworkers, either because of gender, race, or perspective, they may experience pressure to conform with and accept behavior they would otherwise find objectionable to fit in with colleagues and retain their jobs. *See* KATHARINE T. BARTLETT ET AL., GENDER AND LAW 75, 808–14 (Rachel E. Barkow et al. eds., 7th ed. 2017) (quoting Devon W. Carbado & Mitu Gulati, *The Fifth Black Woman*, 11 J. CONTEMP. LEGAL ISSUES 701, 710–15, 717–20 (2001)) (describing "comfort strategies" and "identity performances," in the hypothetical context of black women working in a majority white, male law firm and how these women may conduct themselves, performing their identities in such a way that enables them to fit in with their supervisors and colleagues by, for example, laughing at racist jokes).

34. *Accountable*, *supra* note 7; *see* Jason, *supra* note 13, at 2 (indicating Quinn battled Gamergate harassment throughout 2014).

35. *Accountable*, *supra* note 7.

36. *See infra* notes 37–50 and accompanying text (providing other examples of economic and social harm cyberharassment may cause). A recent incident in the professional gaming community illustrating the interweaving societal issues cyberharassment and doxing cause that may chill speech is the "'Ellie' [s]candal," which arose when a professional male gamer made a new account to play a popular online game, Overwatch. In what he called an "experiment," this player presented himself as a female named Ellie, even going so far as to have girls chat with other players during games to give

Comment has, so far, focused on examples of vicious online harassment women face in the gaming industry, many men also experience severe harassment while gaming online.[37] Women and men in other industries also may experience equally relentless cyberharassment. Women working in other online industries, such as online journalists and web designers, also experience terrible harassment and a general dismissal of their cyberharassment and cyberstalking complaints.[38] Men experience brutal harassment as well, especially in polarized areas such as politics and law enforcement.[39] However, online harassment (and harassment in general)

---

the impression the player was female. Eventually, Ellie was offered a spot on a professional Overwatch team but was harassed and doxed to the point that the account was revealed as fake and Ellie non-existent. While this harassment "would probably not have occurred" if the player was supposedly an anonymous boy rather than a girl, "or at least [it] . . . wouldn't have blown up the way it did[,]" the fact that doxing "worked" in this situation foreshadows future issues for real professional female gamers. Doxers may use the history of unmasking Ellie to justify doxing attempts to "expose" future gamers who present themselves as female. This may endanger females who would like to remain anonymous while they play or may even prevent some females from playing at all. Paul Tassi, *Overwatch's Fake Female Player 'Ellie' Scandal is the Mess that Keeps on Giving*, FORBES (Jan. 6, 2019, 12:29 PM), https://www.forbes.com/sites/insertcoin/2019/01/06/overwatchs-fake-female-player-ellie-scandal-is-the-mess-that-keeps-on-giving/?sh=59231cce28a0 [https://perma.cc/8NXF-BL39].

37. A recent study the Anti-Defamation League conducted indicates 65% of players have experienced "severe harassment" while playing online video games. Severe harassment includes stalking, sustained harassment, and physical threats. Of the people surveyed, 29% revealed experiencing doxing while they played games online. However, 88% of the surveyors noted experiencing positive interactions while playing online games, with 51% saying they have made friends through online gaming. Dave Smith, *Most People Who Play Video Games Online Experience 'Severe' Harassment, New Study Finds*, BUS. INSIDER (July 25, 2019, 10:08 AM), https://www.businessinsider.com/online-harassment-in-video-games-statistics-adl-study-2019-7 [https://perma.cc/U8B2-ESW7]. *See* Jason Hanna & Jamiel Lynch, *An Ohio Gamer Gets Prison Time Over a 'Swatting' Call that Led to a Man's Death*, CNN, https://www.cnn.com/2019/09/14/us/swatting-sentence-casey-viner/index.html [https://perma.cc/KXE3-N6QW] (describing an incident where an argument about a game led a man to make a false report to the police, stating the person he was arguing with had shot his father and was holding his brother and mother hostage; this lead to the death of a man uninvolved in the argument when the police arrived at his house).

38. *See* Emma Marshak, Note, *Online Harassment: A Legislative Solution*, 54 HARV. J. ON LEGIS. 503, 518–20 (2017) (providing examples of female professionals who experienced belittlement (even when one of the women presented evidence of death and rape threats from her harasser), dismissal of their complaints, and challenges in getting help from law enforcement, including claims that law enforcement could do nothing due to jurisdictional issues unless "someone one day put a bullet in [her] brain").

39. The Mayor of San Antonio, Texas, Ron Nirenberg, was recently threatened over Facebook Messenger. Though the incident did not involve doxing or swatting, the online threats were considered dangerous, with the mayor's staff fearing the harasser could be "the next mass shooter[.]" Fares Sabawi, *KSAT 12: 'It's in the Hands of Law Enforcement': Mayor Comments on Suspect's Terroristic Threat Arrest* (ABC television broadcast Oct. 14, 2019), https://www.ksat.com/news/its-in-the-hands-of-law-enforcement-mayor-comments-on-suspects-terroristic-threat-arrest [https://perma.cc/9UQZ-NUZU].

disproportionately affects women and minorities, with many online threats targeting men and (especially) women of color.[40]

Empirical evidence indicates cyberharassment chills speech.[41] Professor Danielle Keats Citron and Jonathon W. Penney state that "[t]he central aim of online abuse is often to silence victims, to punish them for speaking out, and to drive them from public life."[42] Their research shows cyberharassment often achieves its goal, particularly impacting women and marginalized communities and effectively silencing them through online abuse.[43] This, they say, "endangers deliberative democracy, which depends upon contributions from diverse voices and perspectives—particularly groups historically excluded from the 'marketplace of ideas.'"[44] The silencing of women and marginalized groups, therefore, stifles opportunities for these groups as well as growth of the state and nation in general. Professor Mary Anne Franks agrees this online abuse "chills the speech" of its victims.[45] Attorney Carrie Goldberg sees this too, stating victims of doxing and other cyberharassment attacks will "often 'erase themselves.'"[46]

During the 2016 protests surrounding the construction of the Dakota Access Pipeline near the Sioux Tribe Native American Reservation, Ohio troopers who helped in North Dakota had their names withheld "based on reports that law enforcement officers and their families would be targeted for retaliation through doxing if their identities were known." Subsequently, however, a court held, though the request for the officers' names under a public records request was denied by application of the Security Records exception, such exception ended after the troopers returned from their posting at the protests. Gannett GP Media, Inc. v. Ohio Dep't of Pub. Safety, 2017-Ohio-4247, at ¶¶ 28–29, 33–33 (Ohio Ct. Cl. 2017).

40. *See* BARTLETT ET AL., *supra* note 33, at 379 ("Women of color experience disproportionate rates of abuse: they account for 16 percent of the female labor force but 33 percent of women's sexual harassment claims."); *see also* Svana M. Calabro, Note, *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, 61 (2018) ("Online harassers disproportionately target women and people of color, worsening the physical and psychological effects of doxxing and swatting. . . . [P]eople of color are deluged with racially-derogatory harassment online, including frequent references to lynching and slavery. Women of color often face particularly heinous harassment because they are targeted [for] both their race and gender.").

41. Danielle Keats Citron & Jonathon W. Penney, *When Law Frees Us to Speak*, 87 FORDHAM L. REV. 2317, 2319 (2019) (footnote omitted) ("One of us (Penney) has empirically proven, online abuse has a profound 'chilling effect.'").

42. *Id.*

43. *Id.*

44. *Id.* at 2320.

45. *See Feature: SXSW 2019: The Intersection of Law and Technology*, 82 TEX. B.J. 326, 327 (2019) ("Mary Anne Franks, professor of law . . . notes the inability to stop online harassment actually chills the speech of women and minority groups, who are almost exclusively the victims of this type of harassment.").

46. *See id.* (stating victims of online harassment will often "disappear from social media, distance themselves from friends, sometimes drop out of school, and even stop going to family functions").

While Title VII has helped many women and minorities pursue harassment charges in the workplace and access areas of employment previously closed to them,[47] Title VII does not protect women or any other protected group from harassers unrelated to their employer.[48] For this reason, laws like Title VII are unhelpful when cyberharassment prevents women from pursuing emerging avenues of employment and entrepreneurship that are becoming increasingly important and profitable in today's society and economy.[49] Online harassment is often especially intense when aimed at those who work in traditionally white, male-dominated industries.[50] Therefore, victims of cyberharassment must often rely on other federal and state laws to protect them from the dangers of doxing, swatting, and cyberstalking.

Various law journal notes and comments address the need for uniform federal definitions and laws regarding cyberharassment, swatting, and doxing.[51] Uniform federal laws would help standardize divergent state laws and could lead to easier prosecution when jurisdictional issues protect an identified harasser in one state from prosecution in the state where a victim

47. *See* BARTLETT ET AL., *supra* note 33, at 53 ("Title VII . . . prohibits employers from discriminating with respect to the compensation, terms, conditions, or privileges of employment based on the individual's race, color, religion, sex, or national origin.").

48. *Id.* at 409.

49. *See supra* text accompanying notes 16–35 (describing Gamergate's effect on Wu and Quinn's careers, including Wu's withdrawing from a major gaming convention that could have earned her company and game new recognition). *See* Marshak, *supra* note 38, at 509–12 (providing examples where cyberharassment economically harmed women when the harassment infringed upon their work-related online activities). Continuing with the example of the video game industry, in 2019 alone, the United States industry had an economic impact of $90.3 billion. In Texas, the industry added over $4.1 billion to its economy. *The Video Game Industry Economic Growth*, ENT. SOFTWARE ASS'N, https://www.theesa.com/industry/economic-growth/#map [https://perma.cc/354N-M89T].

50. Calabro, *supra* note 40, at 62. *See* BARTLETT ET AL., *supra* note 33, at 378–79 (stating a large percentage of women have experienced sexual harassment at work, with a large percentage of those women being women of color).

51. *See* Lisa Bei Li, *Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting*, 70 FED. COMMC'NS L.J. 317, 323 (2018) ("Given the limitations of state law and the difficulty of regulating online communication, Congress should propose new federal laws to govern actions that perpetuate and result from online harassment—namely, laws dealing with doxing and swatting."); *see also* Calabro, *supra* note 40, at 72 (indicating a cohesive national policy criminalizing swatting and doxing would "ensure a uniform police response to victims' complaints regardless of where the harassment takes place"); Marshak, *supra* note 38, at 523–30 (showing nationally uniform laws, resources, and training materials are the best options for prosecuting cybercrimes because states have divergent laws and state resources).

resides.[52] While this may be true, bills introduced in the United States House and Senate proposing federal regulations for doxing, swatting, and law enforcement training regarding cybercrimes have a slim chance of being enacted or have died altogether.[53] For this reason, Texan lawmakers should consider state legislation regulating cyberharassment and criminalizing doxing and swatting. Texan lawmakers should also consider implementing both continuing law enforcement training and legal education to better prepare law enforcement, judges, and attorneys to handle cyberharassment claims. These programs should use state resources, including research from state schools specializing in cybersecurity and recommendations from professionals regarding how to handle constantly evolving online risks.

In his dissent in *New State Ice Co. v. Liebmann*,[54] Justice Brandeis popularized the thought that in our federal system, a single state, "if its citizens choose, [may] serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."[55] There is a drastic need for cyberharassment regulation, especially for doxing and swatting, and advanced law enforcement training in this area.[56] Judges and attorneys also must be aware of the genuine dangers victims face from cyberharassment, doxing, and swatting.[57] While those in Congress continue

52. *See supra* note 51 (providing examples where three authors recommend uniform federal cyberharassment laws to facilitate prosecution across jurisdictions).

53. Cybercrime Enforcement Training Assistance Act of 2016, H.R. 4740, 114th Cong. (2016), https://www.govtrack.us/congress/bills/114/hr4740 [https://perma.cc/FT27-7GXJ]; Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. (2016), https://www.govtrack.us/congress/bills/114/hr6478 [https://perma.cc/7ZRW-9DJJ]; List of Bills and Resolutions Proposed to Regulate Swatting, GOVTRACK, https://www.govtrack.us/search?q=swatting [https://perma.cc/7J2U-HKZQ] (search for "swatting" in the search box to see a list of current and past proposals for swatting legislation). *See* Anti-Swatting Act of 2019, H.R. 156, 116th Cong. (2019), https://www.govtrack.us/congress/bills/116/hr156 [https://perma.cc/44JR-Q4BJ] (indicating, in 2019, there was a 3% chance that the bill would be enacted); *see also* Preserving Safe Communities by Ending Swatting Act of 2019, H.R. 1772, 116th Cong. (2019), https://www.govtrack.us/congress/bills/116/hr1772 [https://perma.cc/3HW2-HCH3] (indicating, in 2019, there was a 3% chance the bill would be enacted).

54. New State Ice Co. v. Liebmann, 285 U.S. 262 (1932).

55. *Id.* at 311 (Brandeis, J., dissenting).

56. *See supra* notes 12–37 and accompanying text (describing the effects of doxing and swatting on victims and the lack of knowledge law enforcement and judges have regarding these forms of cyberharassment).

57. Such dangers include harm to people's livelihoods and businesses, a loss of peace of mind, and even bodily harm and death. *See* Hanna & Lynch, *supra* note 37 (describing an incident where responding police officers shot and killed a swatting victim). *See generally* Whitford, *supra* note 22 (outlining the harm Brianna Wu experienced due to consistent doxing and cyberharassment, including harm caused to her business when she withdrew from a vital gaming conference where she could

to fight for federal regulation, Texas could be a leader in this area if it passes specific legislation addressing these cyberharassment issues and institutes continuing education programs for law enforcement, judges, and attorneys.

This Comment first lays out the background, history, and analysis of federal and state laws possibly useful to combat doxing, swatting, and other malicious cyberharassment. This section then continues to describe how these laws fail to fully protect cyberharassment victims. In the following section, this Comment will expand on this analysis and recommend courses of action the Texas Legislature may take in addressing and crafting laws proscribing doxing, swatting, and other malicious cyberharassment. This section will use and update language in already existing laws to better address particular issues caused by various forms of cyberharassment. Additionally, this section will include recommendations Texas may consider implementing to educate law enforcement, judges, and lawyers regarding malicious cyberharassment.

IV. BACKGROUND AND HISTORY OF LAWS PERTAINING TO CYBERHARASSMENT

Many critics of proposed laws limiting cyberharassment argue such laws would infringe upon First Amendment free speech rights.[58] Cyberharassers commonly defend themselves by claiming "they are only exercising their First Amendment right to free speech[, a]nd in many cases, an examination of their speech could lead [courts] to concur."[59] However, many scholars agree cyberharassment chills victims' speech when harassment leads victims to withdraw from online forums, society, and even family.[60]

market her game, time spent going over threats with the police, and having to wait in her car while her husband checked their house for intruders).

58. The First Amendment states: "Congress shall make no law . . . abridging the freedom of speech . . . ." U.S. CONST. amend. I. *See* Citron & Penney, *supra* note 41, at 2327 ("Cyberharassment laws are often criticized for chilling speech."); *see also* Julia M. MacAllister, Note, *The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information*, 85 FORDHAM L. REV. 2451, 2463 (2017) ("Challengers to statutory solutions for doxing could raise two primary arguments: (1) that a statute is void for vagueness and (2) that a statute is overbroad by punishing protected speech.").

59. U.S. SENTENCING COMM'N, PUBLIC HEARING ON THE COURT SECURITY IMPROVEMENT ACT OF 2007, at 2 (2009) (providing the written statement of Michael J. Prout, Assistant Director for Judicial Security, United States Marshall Service).

60. *See supra* notes 41–46 and accompanying text (describing evidence that cyberharassment chills victims' speech).

The First Amendment is not an impermeable shield for these harassers. The Supreme Court stated in *Cohen v. California*:[61] "The ability of government, consonant with the Constitution, to shut off discourse solely to protect others from hearing it is . . . dependent upon a showing that substantial privacy interests are being invaded in an essentially intolerable manner."[62] The Court also held a "true threat" is excluded from First Amendment free speech protections.[63] A true threat is a statement "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"; however, "[t]he speaker need not actually intend to carry out the threat."[64] Therefore, the exclusion of true threats from First Amendment protections shields threatened individuals from both the occurrence of threatened violence and from fear of threatened violence and disruption caused by that fear.[65] While a court will look at the totality of the circumstances to determine whether a threat is a true threat, it is still unclear what *mens rea* is required for this designation.[66] In *Elonis v. United States*,[67] the Court held a defendant could be found guilty of issuing a true threat if he "transmits a communication for the purpose of issuing a threat, or with knowledge that the communication will be viewed as a threat."[68] However, though the Court held a finding of negligence would be insufficient *mens rea* in this context, as this could lead a court to hold a defendant guilty of criminal conduct when they are unaware of their wrongdoing, the Court refused to address whether a finding of recklessness would be sufficient.[69] Had the Court addressed this and found recklessness

61. Cohen v. California, 403 U.S. 15 (1971).

62. *Id.* at 21.

63. Calabro, *supra* note 40, at 63; MacAllister, *supra* note 58, at 2464; Marshak, *supra* note 38, at 524; *see* Virginia v. Black, 538 U.S. 343, 359 (2003) ("[T]he First Amendment . . . permits a State to ban a 'true threat.'").

64. *Black*, 538 U.S. at 359–60.

65. *Id.* at 360.

66. MacAllister, *supra* note 58, at 2465–66; *see* SANFORD H. KADISH ET AL., CRIMINAL LAW AND ITS PROCESSES 272 (Rachel E. Barkow et al. eds., 10th ed. 2017) ("The Court [in *Elonis*] made clear that a negligence standard is disfavored in criminal law but did not decide whether recklessness or knowledge was the right mens rea to read into the statute.").

67. Elonis v. United States, 135 S. Ct. 2001 (2015).

68. *See id.* at 2012 (ruling on which *mens rea* standards satisfy the mental state requirements for the Interstate Communications Act (or 18 U.S.C. § 875)).

69. *See id.* at 2011–12 (explaining using a reasonable person standard for the crime would reduce culpability to negligence, a standard the Court has been reluctant to use in criminal statutes, but

to be sufficient *mens rea*, a defendant could be found guilty of issuing a true threat if they were consciously aware of a substantial and unjustifiable risk that could arise from their action (a probability less than substantial certainty), but acted anyway.[70]

A. *Federal Laws*

Though some federal laws could theoretically combat doxing, swatting, and cyberstalking, these laws are often ill-suited to address these issues. The statute addressed in *Elonis*, the Interstate Communications Statute (18 U.S.C. § 875), is a federal law that makes it a crime to "transmit[] in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another."[71] At first glance this seems like a statute victims could use to protect themselves. However, many victims may find the statute vague or underinclusive, given a doxing attack must constitute a "threat to kidnap . . . or . . . injure . . ." to fall under the statute's protection.[72] Additionally, in the wake of *Elonis*, the threat must be a true threat.[73] However, many acts of doxing do not include a definable threat but still are just as terrifying for the victims.[74] One such instance is when a harasser doxes a person, posting the victim's name, address, and other identifiable personal details with a message stoking the rage of others, who will then use those posted details to harass, threaten, swat, or stalk the doxing victim.[75] While the law may hold some of the subsequent harassers accountable for the true threats they make toward the

ultimately declining to address the issue, as neither party in the case argued their side regarding whether recklessness should be the proper standard).

70. KADISH ET AL., *supra* note 67, at 274–75.

71. 18 U.S.C. § 875(c) (1994).

72. *Id.*

73. *See Elonis*, 135 S. Ct. at 2012 ("[T]he mental state requirement in Section 875(c) is satisfied if the defendant transmits a communication for the purpose of issuing a threat, or with knowledge that the communication will be viewed as a threat."); *see also* Virginia v. Black, 538 U.S. 343, 359–60 (2003) (defining a true threat).

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

75. Examples of doxing such as this include "The Zoe Post," in which Zoë Quinn's ex-boyfriend revealed Quinn's personal information and stoked the anger of men who believed women should not play video games or participate in their design. *See* Blanch & Hsu, *supra* note 17, at 3, 7 (describing Quinn's ex-boyfriend's post). *See generally* Malone, *supra* note 8 (providing background regarding Gamergate and the attacks on Quinn).

doxing victim, the law still fails to hold the original doxer responsible for their action if the post was not a definable true threat.[76]

Court interpretation of some statutes—such as the Freedom of Access to Clinic Entrances Act (FACE)—may indicate 18 U.S.C. § 875 could be construed to hold doxers accountable.[77] However, while the Ninth Circuit held doxing health care providers by providing their names and addresses on "'wanted'-style posters constituted a true threat without an additional, specific threat of violence,"[78] it also held this type of threat amounted to a true threat after an attacker killed another physician similarly identified on a "wanted"-style poster.[79] Therefore, this is an unacceptable statute for instances of doxing where the original doxer did not issue an overt threat—victims should not have to wait for another victim to be killed before they may find protection behind this statute.

Another issue affecting the utility of § 875 in combating doxing is the questionable *mens rea* standard that should be applied in the statute.[80] *Elonis*'s holding means lower federal courts may hold the *mens rea* required for § 875 is a purposeful, knowing, or even recklessness standard.[81] This uncertainty may lead lower court judges, especially those ignorant of doxing and swatting's severe implications, to accept the excuse many harassers give

76. Another similar example of doxing includes the doxing of twenty-year-old Joel Vangheluwe, who was falsely identified as the driver who ran over Heather Heyer in Charlottesville, Virginia. Vangheluwe had his information, including his name and address, posted online with text identifying him as the vehicle's owner when he had sold the car years earlier. One post even stated "Killer confirmed" along with his name and address. Vangheluwe v. Got News, LLC, 365 F. Supp. 3d 850, 853–56 (E.D. Mich. 2019). The original doxer's post may not be considered a true threat, as the post would probably not be considered a "statement[] 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." *Black*, 538 U.S. at 359–60.

77. *See* 18 U.S.C. § 248 (1994) (proscribing activities that "by. . . threat of force . . . intentionally . . . intimidates . . . any person because that person is or has been . . . providing reproductive health services" and also creating a private right of action against anyone who by "threat of force . . . intentionally . . . intimidates . . . or attempts to . . . intimidate . . . any person lawfully exercising or seeking to exercise the First Amendment right of religious freedom at a place of religious worship"); *see also* MacAllister, *supra* note 58, at 2470–71 (quoting 18 U.S.C. § 248 (1994)).

78. MacAllister, *supra* note 58, at 2471.

79. Planned Parenthood of Columbia/Willamette, Inc. v. Am. Coal. of Life Activists, 290 F.3d 1058, 1063 (9th Cir. 2002); MacAllister, *supra* note 58, at 2471.

80. *See supra* note 70 and accompanying text (indicating the *Elonis* Court did not address whether recklessness is an appropriate *mens rea* standard under which to assess § 875).

81. *See* Elonis v. United States, 135 S. Ct. 2001, 2012 (2015) (stating "[t]here is no dispute that the mental state requirement in Section 875(c) is satisfied if the defendant transmits a communication for the purpose of issuing a threat, or with knowledge that the communication will be viewed as a threat" but the Court "decline[s] to address" whether a recklessness standard is sufficient).

of simply joking when they make the threats—claiming they were unaware of the dangers or the harm their actions caused.[82]

Another federal law possibly useful in combating doxing and swatting is 18 U.S.C. § 2261A(2).[83] While this statute is slightly more explicit in its prohibition of electronic communication and cyberharassment qualifying as doxing or swatting, the statute's language may still allow harassers to escape prosecution if they can convince judges they were joking and lacked the "intent" to harass or intimidate their target.[84] Additionally, the statute contains language making it difficult to prosecute both doxers who reveal someone's personal information only once and do not engage in the following harassment or threats, and harassers who post one particularly severe post online: the requirement that the actor "engage in a course of conduct."[85] This language indicates a one-off cyberharassment attack, regardless of its severity, may not fall under this statute, as a "course of conduct" means more than one act.[86] A similar problem arises in Texas Penal Code Section 42.07.[87]

---

82. *See supra* text accompanying note 82 (indicating lower court judges may use a purposeful or knowing *mens rea* in applying § 875); *see also infra* note 155 (indicating cyberharassers may claim their actions, including bomb and rape threats, are a "joke").

83. This statute creates a private cause of action for stalking. The relevant part of the statute states:

> Whoever– . . .
>
> (2) with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, *any interactive computer service* or *electronic communication service* or *electronic communication system of interstate commerce*, or any other facility of interstate or foreign commerce to engage in a course of conduct that—
>
> (A) places that person in reasonable fear of the death of or serious bodily injury to a person, a pet, a service animal, an emotional support animal, or a horse . . . ; or
>
> (B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person . . . , shall be punished . . . .

18 U.S.C. § 2261A(2) (2020) (emphasis added).

84. *See infra* notes 155–56 and accompanying text (describing the difficulty in determining a cyberharasser's purpose or knowledge in posting a threat and the danger of a cyberharasser escaping prosecution by claiming he or she was joking).

85. 18 U.S.C. § 2261A(2) (2018); MacAllister, *supra* note 58, at 2474.

86. Blanch & Hsu, *supra* note 17, at 3, 9; *see* Jamie M. McCall & Shawn A. Weede, United States v. Matusiewicz*: Lessons Learned from the First Federal Prosecution of Cyberstalking Resulting in Death*, U.S. ATT'YS' BULL., May 2016, at 17, 22 ("The 'course of conduct' required under the cyberstalking provision (Section 2261(A)(2)) is expressly defined as 'a pattern of conduct composed of 2 or more acts, evidencing a continuity of purpose.'" (quoting 18 U.S.C. § 2266(2) (2012))).

87. *See infra* notes 99–105 and accompanying text (analyzing Texas Penal Code Section 42.07).

B. *Texas Laws*

Various state laws in Texas seem to have aspects useful for doxing or swatting victims, but these laws also fall short. One such law is Texas Penal Code Section 42.07.[88] This law, which the Fourteenth Court of Appeals recently declared unconstitutionally overbroad,[89] outlines and defines criminal "harassment," including when "electronic communication," may be classified as harassment.[90] The currently enacted parts of the Code seemingly most relevant to issues victims of doxing might face include Sections 42.07(a)(1), (2), and (7).[91]

Texas has an explicit harassment statute compared to harassment statutes in some other states, as Section 42.07 particularly addresses and defines electronic communication.[92] However, the composition of the statute creates a few issues regarding interpretation. The first of these issues is both Section 42.07(a)(1) and (2) do not expressly state they apply to electronic communications, whereas Section 42.07(a)(7) does specifically address

88. TEX. PENAL CODE ANN. § 42.07, *declared unconstitutional by* State v. Chen, 615 S.W.3d 376 (Tex. App.—Houston [14th Dist.] 2020, no pet.).

89. *Chen*, 615 S.W.3d at 385.

90. PENAL § 42.07.

91. These sections of the Code are provided below for ease of reference:

> (a) A person commits an offense if, with intent to harass, annoy, alarm, abuse, torment, or embarrass another, the person:
>
> (1) initiates communication and in the course of the communication makes a comment, request, suggestion, or proposal that is obscene;
>
> (2) threatens, in a manner reasonably likely to alarm the person receiving the threat, to inflict bodily injury on the person or to commit a felony against the person, a member of the person's family or household, or the person's property;
>
> . . .
>
> (7) sends repeated electronic communications in a manner reasonably likely to harass, annoy, alarm, abuse, torment, embarrass, or offend another.

Id.

The Texas Legislature has drafted three separate bills that each include a new addition to Section 42.07. Specifically, these bills add a new subsection (8) to Section 42.07(a). Should one of the bills be enacted, the new subsection would likely be relevant to cyberharassment. Tex. S.B. 530, 87th Leg., R.S. (2021); Tex. H.B. 818, 87th Leg., R.S. (2021); Tex. H.B. 2498, 87th Leg., R.S. (2021).

92. *See* PENAL § 42.07(b)(1) (providing a definition and examples of electronic communications); *see also* Natasha N. Phidd, Note, *A Call of Duty to Counterstrike: Cyberharassment and the Toxic Gaming Culture Plaguing Female Gamers and Developers*, 25 WM. & MARY J. RACE, GENDER & SOC. JUST. 461, 470–71 (2019) (stating Texas is the only state out of the three discussed—New York, Washington, and Texas—with a harassment statute explicitly defining electronic communication).

electronic communications.[93] Analyzing this construction, the first two parts of Section 42.07(a) arguably only apply to non-electronic communications, whereas the latter part of the statute specifically applies to electronic communications. However, while criminal statutes not within the penal code must be strictly construed to only proscribe conduct plainly within reach of the statute, with any doubt resolved in the accused's favor, this does not mean the court will ignore the statutory language's plain meaning.[94] Additionally, since Section 42.07 is part of the Texas Penal Code, "[t]he rule that a penal statute is to be strictly construed does not apply" and instead "[t]he provisions of [the] code shall be construed according to the fair import of their terms, to promote justice and effect the objectives of the code."[95]

We can see the legislature knows how to designate "communication" in the statute to including electronic forms, since it specifically refers to this type of communication in the latter part of the statute.[96] The fact that Section 42.07(a)(7)'s text specifies applicability to electronic communication implies there is a divide between the type of behavior proscribed for in-person and electronic communication. The Texas Legislature, if it intended differently, instead could have used "communication" throughout the statute and included a clarification stating reference to communication includes both non-electronic and electronic communication. However, it is possible that, "to promote justice and effect the objectives of the code," the first sections of the statute could be construed to apply to both in-person and electronic communication.[97]

Strictly interpreting Section 42.07's language complicates the prosecution of some cyberharassers. Without addressing the difficulty of determining whether a cyberharasser exhibits a purposeful or knowing *mens rea*, we can see both Section 42.07(a)(1) and (2) seem to address harassment

93. PENAL § 42.07(a).

94. *See* State v. Johnson, 219 S.W.3d 386, 388 (Tex. Crim. App. 2007) (citing Thomas v. State, 919 S.W.2d 427, 430 (Tex. Crim. App. 1996))("[C]riminal statutes outside the penal code must be construed strictly, with any doubt resolved in favor of the accused . . . . But 'strict construction' does not mean that we ignore the plain meaning of the statutory language."); *see also Strict [Literal] Construction*, BARRON'S LAW DICTIONARY (7th ed. 2016) ("A penal statute is generally accorded a strict construction so that only conduct plainly within the reach of the statute is proscribed as criminal."); *cf.* PENAL § 1.05(a) ("The rule that a penal statute is to be strictly construed does not apply to this code.").

95. PENAL § 1.05.

96. *See id.* § 42.07(a)(7) (pertaining to electronic communications).

97. *Id.* § 1.05 ("The provisions of this code shall be construed according to the fair import of their terms, to promote justice and effect the objectives of the code.").

accomplished through threats and inappropriate communications—for example, the exact type of harassment Brianna Wu and Zoë Quinn experienced in Gamergate. However, if these sections of the statute do not apply to electronic communication, then subsections (1) and (2) may not protect victims of cyberharassment. In this case, only Section 42.07(a)(7) may apply to these types of communications.[98]

A few other issues also make it particularly difficult to apply Section 42.07 to protect cyberharassment victims. First of all, the Fourteenth Circuit Court of Appeals, in *State v. Chen*,[99] declared Section 42.07 unconstitutionally overbroad due to "the scope of the statute prohibit[ing] or chill[ing] a substantial amount of protected speech."[100] The court found particular issue with the statute's proscription of electronic communications harassment.[101] It agreed with the analysis that the plain language of the statute endangers constitutional rights of an online critic by exposing her to potential criminal culpability when she simply criticizes another more than once in a way that is embarrassing, annoying, or alarming.[102] Under this analysis, Texas's harassment statute is not narrow enough to protect the First Amendment rights of those who wish to express their displeasure on someone's blog in a way that may simply annoy the blog owner. However, while Texas considers protecting these First Amendment rights, the state should not ignore posts that go a step beyond criticism and become dangerous and malicious cyberharassment.

Analyzing the language in Section 42.07(a)(7), we see another issue in this Section—the same issue present in 18 U.S.C. § 2261A(2)—the requirement that harassing electronic communications be "repeated."[103] This

98. While Section 42.07(a)(1) and (2) proscribe single instances of obscene or threatening communications, these subsections do not indicate that the communication proscribed includes electronic communication, as does Section 42.07(a)(7). *Id.* § 42.07(a).

99. State v. Chen, 615 S.W.3d 376 (Tex. App.—Houston [14th Dist.] 2020, no pet.).

100. *Id.* at 385.

101. *See generally id.* (finding the electronic communications harassment statute unconstitutionally overbroad).

102. *Id.* (quoting *Ex parte* Reece, 517 S.W.3d 108, 111 (Tex. Crim. App. 2017) (Keller, P.J. dissenting)).

103. Similar to 18 U.S.C. § 2261A(2), which requires the accused to "engage in a course of conduct" to proscribe their actions, Texas Penal Code Section 42.07(a)(7) requires the accused to send "repeated electronic communications" to proscribe his or her behavior. 18 U.S.C. § 2261A(2) (2018); PENAL § 42.07(a)(7). Though not the case for all, this type of language is common in many other state harassment statutes, such as those in California and Massachusetts, where "prosecutors . . . have to show repeated attempts of harassment to win a cyberharassment suit." A. Meena Seralathan, Note,

requirement may be an attempt to keep the statute narrow to not curtail protected speech, but it also allows many doxers to escape prosecution. For example, the requirement could permit doxers who post only one or two threats to escape prosecution even if their threats are particularly disturbing or reveal their victims' personal information, exposing them to physical danger. Gamergate victim, Brianna Wu, received a threat exemplifying this situation. It stated: "This means I have to hunt for WU now," and attached a picture taken of her earlier that day by someone around twenty feet away in a crowd.[104] The picture was captioned, "I took a pic earlier," and commentary on the photo stated, "COULDA WENT IN FOR THE KILL."[105]

Similarly, doxers who initially post someone's personal information in an inciteful context but who avoid making any further threats may be able to avoid prosecution under this harassment statute. An example of such a doxer, from *Vangheluwe v. Got New, LLC*,[106] posted "[k]iller confirmed" alongside Jerome Vangheluwe's full name, address, and his (old) license plate number.[107] Doxers posting even a single post like this expose their victims to danger when they incite an online mob's anger and reveal personal information.[108]

While it is important to limit statutes so they do not infringe on First Amendment rights, other limiting language may accomplish this goal while better protecting harassment victims. For example, replacing "repeated" with "severe or pervasive," which is part of the requirement for sexual harassment to be actionable under Title VII, may proscribe more of

Making the Time Fit the Crime: Clearly Defining Online Harassment Crimes and Providing Incentives for Investigating Online Threats in the Digital Age, 42 BROOK. J. INT'L L. 425, 461 (2016).

104. *See* Marshak, *supra* note 38, at 527 (describing a particularly frightening threat Brianna Wu received which indicated the doxing and harassment exposed her to danger).

105. *Id.*

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

107. Id. at 855.

108. *See id.* at 855–56 (relating the Vangheluwes "began receiving countless anonymous threats" after the doxing incident and the threats became so concerning "Michigan State police were notified and the family was warned to leave their home"); *see also* Margaret S. Groban, *Intimate Partner Cyberstalking—Terrorizing Intimate Partners with 21st Century Technology*, U.S. ATT'YS' BULL., May 2016, at 15 (providing reasons the district court gave for varying sentencing upward for a man making advertisements for sexual encounters with his ex-girlfriend, including "the extra danger and fear that [the defendant] caused by using 'anonymous third parties' to harass [his ex-girlfriend], as '[she] ha[d] no idea of the limits they might go to.'" (quoting United States v. Sayer, 748 F.3d 425 (1st Cir. 2014))).

this dangerous cyberharassment.[109] Though the behavior may not be repetitive, it may be considered severe as it exposes victims to physical danger.

The Texas Legislature, as of the time of this writing, is considering three bills that would add a new, eighth subsection to Section 42.07(a).[110] The addition of a new subsection may help solve the issue of the statute being unconstitutionally overbroad by further limiting the current statute.[111] However, every proposed subsection also includes problematic language indicating, for the subsection to apply, the proscribed actions must be repeated.[112] Therefore, regardless of whether the legislature enacts one of these bills, the new bill is not likely to resolve the issue that allows a harasser who posts one severely damaging post to escape prosecution.[113]

Another part of the Texas Penal Code, Chapter 33, covers the topic of computer crimes.[114] While most of this chapter does not address issues addressed in this Comment, Section 33.07, covering online impersonation,

109. *See* Meritor Sav. Bank v. Vinson, 477 U.S. 57, 67 (1986) ("For sexual harassment to be actionable, it must be sufficiently severe or pervasive 'to alter the conditions of [the victim's] employment and create an abusive working environment.'" (quoting Henson v. Dundee, 682 F.2d 897, 904 (11th Cir. 1982) (alteration in original))). Though Title VII is a statute that addresses harassment in a different context from most instances of online harassment this Comment specifically addresses, the inclusion of harassment that is both pervasive (or repetitive) *or* severe is important. Including this language may help people who experience internet hate mobs, such as the mob in Gamergate, bring charges against individuals who may not post more than one or two times, but do post particularly dangerous or threatening posts leading the victims to reasonably fear for their lives or the lives of their loved ones.

110. Tex. S.B. 530, 87th Leg., R.S. (2021); Tex. H.B. 818, 87th Leg., R.S. (2021); Tex. H.B. 2498, 87th Leg., R.S. (2021).

111. One of the bills, S.B. 530, may limit the statute by excluding criminalization of communications "made in connection with a matter of public concern." The bill uses Section 27.001 of the Civil Practice and Remedies Code to define a matter of public concern as:

> a statement or activity regarding:
>
> (A) a public official, public figure, or other person who has drawn substantial public attention due to the person's official acts, fame, notoriety, or celebrity;
>
> (B) a matter of political, social, or other interest to the community; or
>
> (C) a subject of concern to the public

TEX. CIV. PRAC. & REM. CODE ANN § 27.001(7).

112. *See* Tex. S.B. 530, 87th Leg., R.S. (2021) (requiring the electronic communications the subsection proscribes to be "repeated"); Tex. H.B. 818, 87th Leg., R.S. (2021) (requiring the same); Tex. H.B. 2498, 87th Leg., R.S. (2021) (using plurals to indicate proscribed actions, such as "threatening telephone *calls* or other electronic *communications*") (emphasis added).

113. *See supra* text accompanying notes 103–06.

114. *See generally* TEX. PENAL CODE ANN. §§ 33.01–.07 (regulating computer crimes).

may be useful where an attacker intends to harass their victim by making a web page, making a post, or sending an electronic message while "us[ing] the name or persona of another person."[115] Although this would not be useful in many of the doxing instances discussed previously, this statute is applicable when, for example, an attacker makes a fake account on a website, impersonates their victim, and provides the victim's personal information.[116] Depending on whether a telephone call would constitute a "similar communication" under this statute,[117] the statute could also be useful in prosecuting cyberharassers who call the police and, while impersonating their victims, "admit" to participating in a crime, such as an active hostage situation, in order to swat their victim.[118] Cyberharassment is actionable under this statute only if the cyberharasser is impersonating their victims.[119]

While there are no statutes in Texas specifically penalizing doxing the general public,[120] Texas Penal Code Section 38.15 (Interference with Public Duties) protects peace officers and their family members from doxers who

115. *See id.* § 33.07 (proscribing online impersonation undertaken without the impersonated person's consent and with intent to "harm, defraud, intimidate, or threaten" that person).

116. *See, e.g.*, *Ex parte* Dupuy, 498 S.W.3d 220, 223–24 (Tex. App.—Houston [14th Dist.] June 14, 2016, no pet.) (discussing actions the defendant took to impersonate two women online).

117. The statute states "[a] person commits an offense" when a person "sends an electronic mail, instant message, text message, or similar communication" revealing the victim's personal information without the victim's consent, while impersonating the victim in a way that "cause[s] a recipient of the communication to reasonably believe that the other person authorized or transmitted the communication," and with an "intent to harm or defraud any person." This may constitute a third-degree felony if the harasser intends to "solicit a response by emergency personnel." PENAL § 33.07.

118. Two notable instances of swatting where swatters called the police and impersonated their victims include the swatting of twenty-eight-year-old Andrew Finch and of sixteen-year-old Kyle 'Bugha' Giersdorf, the world champion of the popular game Fortnite. In the swatting of Finch, swatters Casey Viner and Tyler Barris (who had mistaken Finch's address for the address of their intended victim) falsely identified themselves as a man at Finch's address who had shot his father and was holding his brother and mother hostage. Police shot and killed Finch when they arrived at his home. Hanna & Lynch, *supra* note 34. In the swatting of Kyle Giersdorf, Giersdorf, who had just won $3 million in the Fortnite World Cup the previous month, was streaming a game live when he left the computer due to a police team arriving at his house. Luckily, Giersdorf was familiar with one of the officers, and the situation ended peacefully. The police stated they responded to a call from someone impersonating Giersdorf, who claimed to be holding his mother hostage after killing his father. Kalhan Rosenblatt, *Fortnite World Champion Kyle 'Bugha' Giersdorf Swatted During Livestream*, NBC NEWS (Aug. 13, 2019, 7:23 AM), https://www.nbcnews.com/news/us-news/fortnite-world-champion-kyle-bugha-giersdorf-swatted-during-livestream-n1041736 [https://perma.cc/3956-D3AZ].

119. *See* PENAL § 33.07 (proscribing actions constituting online impersonation).

120. TEXAS GUIDE, *supra* note 15, at 2 (stating the legality of doxing and swatting is "not clearly established").

undertake cyberattacks to interfere with police duties.[121] As this only applies to peace officers, the statute does not help private citizens who experience doxing, but it does indicate the legislature is aware of the dangers such cyberattacks may pose.

V. ANALYSIS

Cyberharassment—including doxing and swatting—has gained an increasing amount of attention both nationally and in Texas, but laws are falling behind developments in technology and electronic communication.[122] States may have their own laws addressing these types of cyberharassment, but even those laws are often underdeveloped, as the concepts of doxing and swatting are relatively new territory for lawmakers and law enforcement.[123]

Though the Texas Department of Information Resources recognizes doxing can be dangerous and even deadly, especially when it enables the act of swatting, the department also realizes the legality of the acts "is not clearly established and varies across jurisdictions."[124] This Comment urges Texas to criminalize doxing and swatting when one may consider these actions a true threat by drafting a new statute specifically addressing these two forms of cyberharassment. This Comment also urges Texas courts to consider accepting the use of a recklessness standard to assess whether a threat is a true threat. After accepting this standard, courts should also consider

121. *See* PENAL § 38.15(a)(1), (d), (d-1) (stating in Section 38.15(a)(1): "A person commits an offense if the person with criminal negligence interrupts, disrupts, impedes, or otherwise interferes with . . . a peace officer while the peace officer is performing a duty" and adding in Section 38.15(d-1) that "there is a rebuttable presumption that the actor interferes with a peace officer if it is shown . . . that the actor intentionally disseminated the home address, home telephone number, emergency contact information, or social security number of the officer or a family member of the officer").

122. *See, e.g.*, *A Look at the Legal Consequences of Swatting After Police Shoot Innocent Man*, NPR (Jan. 2, 2018, 4:13 PM), https://www.npr.org/2018/01/02/575168288/a-look-at-the-legal-consequences-of-swatting-after-police-shoot-innocent-man [https://perma.cc/NR2K-2J8Q] [hereinafter *Legal Consequences of Swatting*] (interviewing Professor Neal Katyal from Georgetown University about the legal difficulties authorities came across in prosecuting the perpetrators in the deadly swatting of Andrew Finch, stating "[t]he law hasn't totally caught up to this type of thing" and that authorities seemed to struggle with how to categorize the crime, as there are no federal swatting laws and murder is quintessentially a state crime).

123. *See id.* (explaining swatting does not usually result in death as it did in the swatting of Andrew Finch, so state swatting laws, such as California's, may not capture the gravity of the crime since the laws may not address different degrees of swatting).

124. *See* TEXAS GUIDE, *supra* note 15, at 1 (addressing the dangers of doxing and swatting and referring specifically to the fatal swatting case in Kansas).

finding a harasser guilty of issuing a true threat when the harasser recklessly doxes someone by providing a victim's personal information, such as his name and address, in a context that may place the victim in physical danger. Using a recklessness standard would allow Texas courts to hold cyberharassers accountable for posts or actions if they were consciously aware of a substantial and unjustifiable risk of harm their actions could cause, but they acted anyway.[125]

Lawmakers may also consider statutes contemplating different degrees of doxing and swatting since some instances do not cause much harm, as in the swatting of Kyle Giersdorf,[126] while others may lead to physical harm or even a victim's death, as in the swatting of Andrew Finch.[127] Finally, Texas should consider instituting continuing education programs for law enforcement, judges, and lawyers. The programs would educate these groups about changes in technology and cyberharassment, as many in these professions fail to understand technological changes, how much people put on the internet, and how this information may potentially be used against them.[128]

A. *Analyzing the Complexities of Doxing and Cyberharassment Constituting a "True Threat"*

Though doxing is a relatively new concept, the practice of posting people's personal information on the internet, as well as the term itself, came about in the 1990s, or at least the mid-2000s.[129] Doxing has been used for both seemingly justifiable reasons as well as to terrorize and harass, and as a result, people understand doxing in various ways.[130] For that reason,

125. *See* KADISH ET AL., *supra* note 67, at 274–75 (defining "recklessness").

126. *See generally* Rosenblatt, *supra* note 119 (describing the swatting of Kyle Giersdorf).

127. *See generally* Hanna & Lynch, *supra* note 37 (describing the swatting of Andrew Finch).

128. Telephone Interview with Dr. Greg White, Director, Cent. for Infrastructure Assurance & Sec. at the Univ. of Tex. at San Antonio, & Julina Macy, Media Relations, Ctr. for Infrastructure Assurance & Sec. at the Univ. of Texas at San Antonio (Nov. 14, 2019) [hereinafter White] (speaking about how many professionals and law enforcement do not realize how much information younger generations put on the internet and how that information may be used against them).

129. *See* Megan Garber, *Doxing: An Etymology*, ATLANTIC (Mar. 6, 2014), https://www.theatlantic.com/technology/archive/2014/03/doxing-an-etymology/284283/ [https://perma.cc/XQ27-V6XS] (stating people began to post fellow users' personal information as a form of retaliation on Usenet, a discussion board, in the 1990s, "with the term 'dox' . . . [referring] to identity-revelation—seem[ing] to" come into usage by the late 2000s).

130. *See id.* (explaining there is a variation in how people see doxing, using the example of journalists seeing doxing as (generally) a good thing due to the goal of many journalists to reveal "previously unknown information").

doxing can be a complex topic and, in some circumstances, may even seem justified.[131] Thus, doxing should be assessed to see whether posting someone's information may constitute a true threat to the doxing victim. Using such an assessment would protect constitutionally protected speech from proscription while protecting doxing victims from legitimate threats of danger.[132]

1. Considering the Context of a Post May Enable Judges to Determine Whether a Post Was a "True Threat"

Though doxing was used early on "as a retaliation mechanism during arguments," it has been used for seemingly beneficial reasons. One such instance includes the outing of notorious Reddit troll Michael Brutsch (AKA "Violentacrez"),[133] who was well-known for his offensive posts, especially those including pictures of scantily clad teenage girls (taken from the girls' Facebook accounts), in a section with around 20,000 subscribers titled *Jailbait*.[134] Regardless of doxing's potential benefits, the practice invites danger, especially when harassers post personal information that incites the rage of people who may decide to punish the doxing victim. This sort of vigilantism, though perhaps well intentioned, may even reveal innocent people's information when harassers mistakenly identify them as targets. An example of a misidentified doxing target is Joel Vangheluwe, who was mistakenly named as the killer of Heather Heyer, who tragically died when a car rammed into a crowd in Charlottesville, Virginia.[135] Before

131. *See infra* notes 134–35 and accompanying text (providing an example of what some may consider a positive instance of doxing in revealing Michael Brutsch as the Reddit user "Violentacrez").

132. *See* Gretchen C. F. Shappert, Elonis v. United States: *Consequences for 18 U.S.C. § 875(c) and the Communication of Threats in Interstate Commerce*, 64 U.S. ATT'YS' BULL. 30, 30, 35 (2016) (citing Watts v. United States, 394 U.S. 705, 707 (1969) (per curiam)) (indicating a threat statute interpreted to reach only a true threat does not reach constitutionally protected speech).

133. *See* Garber, *supra* note 130 (giving examples of the variation in how people see doxing and stating even some Reddit users "applauded the Gawker reporter Adrian Chen's outing of Violentacrez," a notorious Reddit user).

134. Adrian Chen, *Unmasking Reddit's Violentacrez, the Biggest Troll on the Web*, GAWKER (Oct. 12, 2012, 4:00 PM), https://gawker.com/5950981/unmasking-reddits-violentacrez-the-biggest-troll-on-the-web [https://perma.cc/3XMJ-8W6V] (revealing Violentacrez posted porn, descriptions of himself having oral sex with his nineteen-year-old step-daughter, pictures taken covertly in public of women's breasts or backsides, as well as pictures of scantily-clad teenagers taken from their personal social media pages).

135. *See generally* Vangheluwe v. Got News, LLC, 365 F. Supp. 3d 850, 853–56 (E.D. Mich. 2019) (describing the doxing of Jerome Vangheluwe and his twenty-year-old son Joel, who was mistakenly named as the driver of the car that hit and killed Heather Heyer).

the confusion was settled, the Michigan State police warned the Vangheluwe family to leave their home in the wake of receiving online threats after doxing revealed their home address.[136] The fear the Vangheluwes and the police experienced is the same fear many of the women involved in Gamergate experienced in the wake of receiving graphic online threats detailing their rape or death—fear some unknown person was lurking nearby to attack the victim for whatever initially sparked the doxers' rage.[137] This fear is not unfounded given the uptick in mass shootings and threats, including bomb threats, which are often preceded by rage-filled social media postings or emails.[138]

The type of doxing the Vangheluwes and the victims of Gamergate experienced, however, is distinguishable from the outing of Violentacrez as Michael Brutsch.[139] Important differences between Adrian Chen's actions and those of the Gamergate and Vangheluwe doxers include: the context in which the doxers posted victims' personal information; the level of detail in the information they included and the care with which they posted the information; and their personal qualifications and reasons for posting.

For example, Adrian Chen, a writer for the blog *Gawker*, spoke with Violentacrez before posting his article and only revealed the man's name and the city in which he lived, not his specific address or other intensely

136. *Id.* at 856.

137. *See, e.g.*, Whitford, *supra* note 22 (describing the effect doxing had on Brianna Wu, leading her to lock rooms in her house, such as the attic and basement, with a padlock).

138. Another victim of Gamergate harassment was Anita Sarkeesian, who was forced to cancel a lecture she planned to give at Utah State University after someone sent a bomb threat to the university before the event and said in an email, "I have at my disposal a semi-automatic rifle, multiple pistols, and a collection of pipe bombs . . . ." The email continued, threatening Sarkeesian personally: "I will write my manifesto in her spilled blood, and you will all bear witness to what feminist lies and poison have done to the men of America." Edwards, *supra* note 15. *See* Sarah N. Lynch & Mark Hosenball, *Stopping America's Next Hate-Crime Killers on Social Media Is No Easy Task*, REUTERS (Aug. 9, 2019, 5:10 AM), https://www.reuters.com/article/us-usa-shooting-internet/stopping-americas-next-hate-crime-killers-on-social-media-is-no-easy-task-idUSKCN1UZ10S [https://perma.cc/XT4N-T3KW] (stating hate-filled online posts often precede racially motivated shootings). *See generally* Jason Silverstein, *There Were More Mass Shootings than Days in 2019*, CBS NEWS (Jan 2, 2020, 11:45 AM), https://www.cbsnews.com/news/mass-shootings-2019-more-than-days-365/ [https://perma.cc/W5 88-XPTD] (stating in 2019 there were 417 mass shootings in the United States—or shootings of at least four people at a time, excluding the shooter—with thirty-one of those 417 shootings constituting mass murders).

139. *See generally* Chen, *supra* note 135 (describing Chen's process in discovering and revealing the identity of Reddit user "Violentacrez").

personal details.[140] According to Chen, the biggest fear Brutsch expressed regarding the impending revelation of his identity was the possible loss of his job.[141] Chen's journalistic post, therefore, was not nearly as invasive as the Vangheluwe post. Therefore, it is unlikely it would be considered a true threat because Chen did not reveal the information in a way that was designed to incite readers to attack Brutsch. However, the result might have differed if Chen posted the article in a context analogous to how the Vangheluwes' information was posted—on Twitter and Facebook, addressing people who knew the parties attacked in Charlottesville, with a clear message directly linking Vangheluwe to the attack.[142] A hypothetical illustrates this point: If Chen had instead outed Brutsch as Violentacrez in a context such as a Facebook post directed at parents of young teenage girls, the post may more likely qualify as a true threat.[143] In this context, though a threat may not be overt, the context itself may be considered an implied threat, as it would seemingly aim to incite the anger of those parents and encourage them to personally find and exact revenge against Brutsch, using the personal information provided in the post to do so.

A doxing statute should consider the act of doxing someone's information in an inciting or threatening context, without a further overt threat, as a true threat. Such doxing would fall under an exception from First Amendment protections[144] because the threat is clearly implied.[145] Such a statute would proscribe posting someone's personal information in a carefully selected context where a chosen group of people would see it and

140. *See id.* (revealing the author of the blog spoke with the subject of his doxing, Michael Brutsch, before he posted his article on *Gawker* revealing Brutsch as a forty-nine-year-old man from Arlington, Texas).

141. *Id.*

142. *See* Vangheluwe v. Got News, LLC, 365 F. Supp. 3d 850, 854–55 (E.D. Mich. 2019) (providing examples of doxing that took place on Twitter and Facebook).

143. *Cf.* Virginia v. Black, 538 U.S. 343, 359–60 (2003) (defining a true threat as "statement[] 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").

144. Calabro, *supra* note 40, at 63; MacAllister, *supra* note 58, at 2464; Marshak, *supra* note 38, at 524; *see Black*, 538 U.S. at 359 ("[T]he First Amendment . . . permits a State to ban a 'true threat.'" (quoting Watts v. United States, 394 U.S. 705, 708 (1969) (per curiam))).

145. Justice Alito comments in his dissent in *Elonis* that "context matters" when assessing whether statements should be considered threats. He says:

> Statements on social media that are pointedly directed at their victims, by contrast, are much more likely to be taken seriously. To hold otherwise would grant a license to anyone who is clever enough to dress up a real threat in the guise of rap lyrics, a parody, or something similar.

Elonis v. United States, 135 S. Ct. 2001, 2016 (2015) (Alito, J., dissenting).

where the details the harasser provides are reasonably certain to, and do, incite the harasser's audience to use the posted information to seek out the victim, threaten her, and place her in physical danger. An example of a situation where a harasser doxed his victims in a particular context and consequently exposed the victims to physical danger is addressed in *Ex parte Dupuy*,[146] a 2016 Texas case. In this case, a man created fake accounts on adult websites and doxed two women by providing their personal information in an advertisement for a female escort.[147]

It may be difficult to determine whether a statement or post is an implied threat; the determination would depend on a judge's specific assessment of the post's context. However, by considering posts that are implied threats to be true threats, courts would allow prosecution in situations where a post is clearly an attack on a victim, such as in *Ex parte Dupuy*, where a harasser uses a particular group on the internet as his or her weapon.[148]

2. Using the *Mens Rea* Standard of Recklessness When Assessing a "True Threat" Will Help Prosecute Doxers Who Claim the Threat Was a "Joke"

To help address the harms malicious doxing causes, both federal and Texas courts should consider accepting the *mens rea* standard of recklessness when assessing whether a threat is a true threat. Adopting this standard would allow prosecution of doxers and other harassers when the prosecution cannot prove it was the doxers' "conscious object" to harm their victims or that they were aware their conduct would be practically

146. *Ex parte* Dupuy, 498 S.W.3d 220 (Tex. App.—Houston [14th Dist.] 2016, no pet.) (outlining how a cyberharasser posted women's information on adult websites).

147. *See Ex parte* Dupuy, 498 S.W.3d at 231 (stating the poster's conduct "exposed the [victims] to danger" when he placed fake female escort advertisements on an adult website and put the two women's names and phone numbers together on the advertisements in such a way that anyone could confirm the phone numbers belonged to the two women). A federal case with similar facts also found such doxing exposed a woman to danger when her harasser posted her information in a fake advertisement. This advertisement included photos of the victim from before her relationship with her harasser ended, step-by-step instructions on how to get to the woman's home, and "a list of sexual acts [that] she [would] . . . perform." *See* Groban, *supra* note 106, at 14–15 (quoting United States v. Sayer, 748 F.3d 425, 437 (1st Cir. 2014)) (stating the court considered the action dangerous due to the defendant's "using 'anonymous third parties' to harass [his ex-girlfriend], as [she] 'had no idea of the limits they might go to'").

148. *See generally Ex parte* Dupuy, 498 S.W.3d 220 (presenting facts where a harasser posted his victims' information in an adult advertisement, exposing them to strangers who could use the information to find them).

certain to bring about harm.[149] It is often challenging for the prosecution to prove these mental states,[150] so using "purpose" and "knowledge" as the *mens rea* requirements for finding a true threat may ultimately leave victims open to severe, malicious doxing without hope of redress.[151] In *Elonis*, the Court stated it "has long been reluctant to infer that a negligence standard was intended in criminal statutes"[152] and explicitly held negligence is insufficient *mens rea* to find a suspect guilty of issuing a true threat.[153] For these reasons, using a "recklessness" *mens rea* standard, which allows holding a defendant culpable for an action if they were consciously aware of a substantial and unjustifiable risk of harm, but acted anyway,[154] may help prosecute harassers who claim their actions are a joke to escape culpability.[155]

149. *See* KADISH ET AL., *supra* note 67, at 274 (describing the *mens rea* standards of purpose and knowledge).

150. *See* Nancy Leong & Joanne Morando, *Communication in Cyberspace*, 94 N.C. L. REV. 105, 109 (2015) (stating actual knowledge, in many instances, is difficult for the prosecution to prove).

151. During Gamergate, the FBI tracked down some of the doxers who participated in the threats issued to women like Quinn and Wu. One such man was "linked to dozens of rape, bomb, and death threats targeting women involved in the video game scene." After the FBI showed him a threatening email connected to him, the suspect admitted sending it and "confessed that he knew it was . . . 'a federal crime to send a threatening communication to anyone and [would] never do it again . . . .'" However, despite the "email trail, a confession, and an admission from the suspect that he knew he was breaking the law" the suspect claimed his threat was a "joke" and escaped prosecution. *See* Edwards, *supra* note 15 (describing the FBI investigation of Gamergate). Under a purposeful or knowing *mens rea* standard, doxers could likely escape prosecution by claiming their actions are a joke and do not demonstrate the requisite conscious object to cause harm to their victims or the requisite awareness that their conduct would be practically certain to bring about such harm. *See* KADISH ET AL., *supra* note 67, at 274 (describing the *mens rea* standards of purpose and knowledge).

152. *Elonis*, 135 S. Ct. at 2004 (quoting Rogers v. United States, 422 U.S. 35, 47 (1975)) (Marshall, J., concurring) (alterations in original).

153. *See id.* at 2012–13 (stating while "the mental state requirement in Section 875(c) is satisfied if the defendant transmits a communication for the purpose of issuing a threat, or with knowledge that the communication will be viewed as a threat[,] . . . negligence is not sufficient to support a conviction under Section 875(c)").

154. *See* KADISH ET AL., *supra* note 67, at 274–75 (describing the *mens rea* standard of recklessness).

155. This sort of situation seemed to concern Justice Alito, who commented in his *Elonis* dissent that context matters when assessing whether a statement on social media directed at a victim should be considered a threat. He stated:

> Statements on social media that are pointedly directed at their victims . . . are much more likely to be taken seriously. To hold otherwise would grant license to anyone who is clever enough to dress up a real threat in the guise of . . . a parody, or something similar.

Elonis, 135 S. Ct. at 2016 (Alito, J., dissenting). Using the example of the Gamergate doxer who escaped prosecution for rape, bomb, and death threats by claiming his actions were a joke, it is apparent

3. A Statute Proscribing Doxing Would Fit in with Other Texan Laws Regarding Harassment and Computer Crimes

A statute proscribing posts that reveal or use personally identifiable information to threaten or intimidate the identified person would align with current Texas statutes regarding computer crimes. This includes Section 33.07, which regulates a person's behavior when they use another's name or persona online in a criminal, non-consensual way.[156] In the Texas Court of Appeals case *State v. Stubbs*,[157] the Fourteenth District stated Section 33.07 was constitutional under a First Amendment challenge.[158] While the court does indicate speech intended merely to hurt someone's feelings is protected, speech intending to intimidate or threaten is more likely to fall outside of First Amendment protections.[159] True threats or "statements 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" is another category of speech that falls outside of these protections.[160] Intimidation is also a type of true threat "where a speaker directs a threat to a person or group of persons with the intent of placing the victim in fear of bodily harm or death."[161] The court stated: "There is no dispute that the Legislature legitimately may punish 'threatening' and 'intimidating' speech involving physical harm or violence."[162] The court continued, stating such an act, "whether or not the actor actually produces fear of bodily injury in another, is a socially

using a recklessness standard may have allowed for his prosecution because the doxer admitted the threats were a federal crime and acted anyway. Edwards, *supra* note 15.

156. *See* TEX. PENAL CODE ANN. § 33.07 ("A person commits an offense if the person, without obtaining the other person's consent and with the intent to harm, defraud, intimidate, or threaten any person, uses the name or persona of another person to: (1) create a web page on a commercial social networking site or other Internet website; or (2) post or send one or more messages on or through a commercial networking site or other Internet website, other than on or through an electronic mail program or message board program.").

157. State v. Stubbs, 502 S.W.3d 218 (Tex. App.—Houston [14th Dist.] 2016, pet. ref'd).

158. *See generally id.* at 227–37 (concluding the statute is constitutional under the First Amendment by analyzing "the specific types of criminal intent delineated by the statute and the conduct such intent requirements seek to proscribe," determining whether the statute was content-based or content-neutral, overbroad, and impermissibly vague).

159. *Id.* at 228–29.

160. *Id.* at 227–28 (quoting Virginia v. Black, 538 U.S. 343, 359 (2003)).

161. *Id.* at 228 (quoting *Black*, 538 U.S. at 360).

162. *Id.*

intolerable type of conduct or 'wrong' that implicates society's interest in establishing criminal laws."[163]

Though Texas Penal Code Section 33.07 does cover a different type of computer crime, online impersonation (which may, at times, apply to *specific* doxing and swatting instances).[164] However, the statute serves a similar purpose—preventing someone from using another's personal information in an electronic context to harm them—and would prevent similar harms as a statute criminalizing doxing.[165] For this reason, extending protections similar to Texas Penal Code Section 33.07 to situations when doxed individuals are not being impersonated is not far-fetched for the Texas Legislature.

The Fourteenth District also found in *Ex parte Dupuy*, addressing Section 33.07, an online offense cannot be excused as "non-violent" or "virtual-based" conduct when it exposes victims to danger.[166] In this case, one of the victims started receiving numerous phone calls and text messages from people who got her information from an escort ad on an adult website, which provided her phone number, a fictional rate for her services, and multiple pictures.[167] The man who posted the ads attempted to characterize the ads as "the functional equivalent of electronically posting 'for a good time call (*insert name*)[,]'" and therefore were "'non-violent' and 'virtual-based.'"[168] Despite this argument, the court held because the ads displayed the victims' real names, phone numbers, and photos, and anybody who obtained this personal information could confirm it was accurate, the

163. *Id.*

164. *See* TEX. PENAL CODE ANN. § 33.07 (making it an offense to "use[] the name or persona of another . . . without obtaining the person's consent and with the intent to harm").

165. *See Stubbs*, 502 S.W.3d at 236–37 (stating "the Legislature's intent [is] to target more intense rather than less intense mental states" regarding the statute stating a person commits an offense when someone impersonates someone online "with the intent to harm, defraud, intimidate, or threaten any person").

166. *See Ex parte* Dupuy, 498 S.W.3d 220, 231 (Tex. App.—Houston [14th Dist.] 2016, no pet.) (stating the appellant's conduct in placing fake advertisements on an adult escort site for two women and putting their names and phone numbers together on those advertisements "exposed the [victims] to danger" because "[t]he phone numbers in those searches belonged to [the two women], respectively[, and i]f appellant could confirm their phone numbers through an Internet search, so could anybody who obtained their names and phone numbers from the ads").

167. *See id.* at 224 (describing the ads a man created for two women as revenge for the women breaking up with him).

168. *Id.* at 231.

trial court could reasonably conclude the ads exposed the victims to danger.[169]

This parallels situations a doxing victim may experience. Though most Gamergate victims and the Vangheluwes did not have their harassers impersonate them when they were doxed, their personal information was placed in contexts where people who felt negatively about the individuals could view it.[170] Thus, a court may conclude posting a victim's information in such a context similarly exposes victims to danger—people could just as easily act on information the Gamergate and Vangheluwe doxers posted as information provided by the defendant in *Ex parte Dupuy*.

Additionally, Texas recently enacted a law criminalizing student cyberbullying.[171] "David's Law," named in honor of a young San Antonio teen, David Molak, who committed suicide in 2016 after suffering from extreme cyberbullying and online harassment, went into effect on September 1, 2017.[172] The law greatly expanded the power of school districts, law enforcement, and courts to pursue cyberbullying claims, even going so far as to allow courts to "issue subpoenas and uncover people who are posting anonymously online" due to the State classifying cyberbullying as a misdemeanor.[173] The law also made changes to Texas Penal Code Section 42.07, the Harassment Statute, to more explicitly include online

169. *See id.* ("The trial court could reasonably . . . find . . . the ads exposed the complainants to danger.").

170. Doxers and people who feel negatively about doxing targets may see posts made about targets and respond within a matter of minutes. For example, actress and gamer, Felicia Day, was terrified of having her information doxed and was hesitant to post about Gamergate due to her fear. Just minutes after she made her first public post about Gamergate, merely expressing her terror at the thought of being doxed and commenting on her fear of posting on the subject, someone posted what they asserted was her email and address in the comments below the post. Alex Hern, *Felicia Day's Public Details Put Online After She Described Gamergate Fears*, GUARDIAN (Oct. 23, 2014, 8:18 AM), https://www.theguardian.com/technology/2014/oct/23/felicia-days-public-details-online-gamergate [https://perma.cc/F6JC-N7GJ]. *See supra* note 143 and accompanying text (describing the context in which the Vangheluwes's information was doxed).

171. *See* Benson Varghese, *Nine Things You Need to Know About Texas' New Cyberbullying Law*, JURIST (Aug. 30, 2017, 5:44 PM), https://www.jurist.org/commentary/2017/08/benson-varghese-cyberbully-texas/ [https://perma.cc/B65C-BQ32] (stating David's Law, signed into law on June 9, 2016, makes "cyberbullying . . . officially . . . illegal in Texas" and addresses how "[i]n the past, there was little law enforcement and school districts in Texas could do to deter cyberbullying").

172. *See id.* (providing information about David's Law and stating the law "goes into effect on September 1, 2017" (this article was written in August of 2017 before the law went into effect)).

173. *See David's Law: Preventing Cyberbullying in Texas Schools*, FRISCO ISD, https://www.friscoisd.org/docs/default-source/guidance-and-counseling/davidslaw.pdf [https://perma.cc/X9Z3-RLJQ] (describing the implications of Senate Bill 179 classifying cyberbullying as a misdemeanor).

communication tools used to facilitate cyberbullying.[174] Although David's Law is a vast improvement in the area of online harassment and bullying, as previously school districts and law enforcement could do little to deter cyberbullying, this law is still not enough to deter harassment similar to what the Vangheluwes and Gamergate victims experienced because it only applies to school-related bullying.[175] Additionally, David's Law would not apply to cyberharassment targeting people over the age of eighteen.[176] These changes updated Texas's cyberharassment laws, which is a giant first step toward further updating laws to keep up with technology and electronic communication. Texas's familiarity with and willingness to take steps to criminalize cyberbullying indicates the state may be ready to criminalize doxing and swatting, two similarly dangerous forms of online abuse.

B. *The Absence of a Law Specifically Addressing Swatting Should Be Rectified to Avoid Potential Problems in Classifying Such Crimes*

Swatting is becoming increasingly common and may occur in private households, elementary schools, secondary schools, convention centers, arenas, and colleges.[177] Though the State of Texas realizes swatting is dangerous, deadly, and ill-motivated, the legality of the act is still not clearly established.[178] As the legality of swatting varies across jurisdictions, prosecuting swatters may prove difficult, especially when done across jurisdictional lines, as in the case of Andrew Finch.[179] Professor Neal Katyal stated, "[t]he law hasn't totally caught up to this type of thing" and discussed how authorities in the case seemed to struggle with how to categorize the crime, as there are no federal swatting laws. Complicating factors included how Andrew Finch was killed in Kansas, but

174. *See SB 179—David's Law: 85th Texas Legislative Session*, EDUC. SERV. CTR., REGION 20, https://www.esc20.net/page/open/47320/0/David_s_Law_Overview.pdf [https://perma.cc/3RRM-ARFW] [hereinafter *SB 179*] (stating "David's Law changes Section 42.07 . . . to more fully and clearly include the modern Internet-based communication tools and methods perpetrators use to cyberbully their victims").

175. *See* Varghese, *supra* note 171 ("David's law doesn't apply to workplace bullying[, i]t pertains to student bullying . . . .").

176. *See generally SB 179*, *supra* note 174 (indicating David's Law applies only to minors and prohibits cyberbullying that relates to, interferes with, or disrupts a student's schooling).

177. Laura-Kate Bernstein, *Investigating and Prosecuting "Swatting" Crimes*, U.S. ATT'YS' BULL., May 2016, at 51, 52.

178. TEXAS GUIDE, *supra* note 15, at 1–2.

179. *See Legal Consequences of Swatting*, *supra* note 123 (indicating the call in the swatting-related death of Andrew Finch came from Los Angeles, California and was made to police in Wichita, Kansas).

the call came from California; and murder is quintessentially a state crime.[180] Though swatting laws do not exist in all states,[181] Professor Katyal indicated existing state swatting laws may be underdeveloped to sufficiently address all situations.[182] For this reason, Professor Katyal suggested federal and state legislatures consider swatting statutes that "think through the degrees of swatting,"[183] as swatting may be diffused peacefully as it was in the swatting of Kyle Giersdorf,[184] or it may result in death, as in the swatting of Andrew Finch.[185]

Texas should learn from California's difficulty in characterizing the swatting crime in the Finch case and institute a law criminalizing not only swatting but also addressing different degrees of swatting. These degrees may range from swatting that: (1) results in death, (2) results in injury, and (3) is peacefully diffused. Doxing statutes may also be broken down into degrees, as doxing may often lead to swatting or similarly place victims in danger.[186] For example, doxing degrees could mirror a swatting statute by addressing doxing that: (1) results in death, (2) results in injury, or (3) results in the unauthorized revelation of personally identifiable information that exposes the target to risk of physical danger.

---

180. *Id.*

181. *See* TEXAS GUIDE, *supra* note 15, at 2 (stating the legality of swatting is "not clearly established and varies across jurisdictions").

182. *See Legal Consequences of Swatting*, *supra* note 123 (indicating though California has a swatting statute, it may not capture the gravity and tragedy of the resultant death from this particular instance of swatting because swatting does not usually result in death).

183. *Id.*

184. Telephone Interview with Professor Robert Summers, Professor of Law, St. Mary's Sch. of Law (Nov. 26, 2019); *see, e.g.*, *A Look at the Legal Consequences of Swatting After Police Shoot Innocent Man*, NPR (Jan. 2, 2018), https://www.npr.org/2018/01/02/575168288/a-look-at-the-legal-consequences-of-swatting-after-police-shoot-innocent-man [https://perma.cc/NR2K-2J8Q] (providing a statement by Professor Neal Katyal of Georgetown University stating "the law hasn't totally caught up to this type of thing" concerning the swatting-related death of Andrew Finch). *See, e.g.*, Rosenblatt, *supra* note 119 (stating Giersdorf was able to diffuse the situation quickly due to his knowing one of the responding officers).

185. *See, e.g.*, *Legal Consequences of Swatting*, *supra* note 121 (concluding swatting led to Andrew Finch's death).

186. *See Ex parte* Dupuy, 498 S.W.3d 220, 231 (Tex. App.—Houston [14th Dist.] 2016, no pet.) (explaining how a harasser's conduct in placing two women's personal information on an adult escort site "exposed the [victims] to danger"); *see also* TEXAS GUIDE, *supra* note 15, at 1(stating doxing may enable swatting).

C. *Changing Language in Harassment Statutes Proscribing "Repeated" Electronic Communications to Language Proscribing Severe* or *Repeated Actions May Prevent Malicious Cyberharassers from Escaping Prosecution*

Harassment statutes across the United States vary in how they define conduct sufficient for prosecution,[187] with many states, including Texas, requiring electronic communications be repeated.[188] This requirement, however, may allow doxers who post only one or two threats to escape prosecution. When such threats are particularly disturbing or expose victims' personal information in contexts that may put the victim in physical danger, such harassment statutes will not provide respite.[189] For this reason, the Texas Legislature may consider crafting a new statute proscribing malicious cyberharassment, doxing, and swatting, or at least changing the language in the current harassment statute—specifically Section 42.07(a)(7)—to encompass both severe *or* repeated actions, similar to the language employed in Title VII.[190]

While the Fourteenth Circuit recently declared Texas's current harassment statute unconstitutionally overbroad, defining vague words in the statute may help narrow it down.[191] Words that seem the most troubling, and that the statute should potentially define, include "alarm" and

187. *See* Seralathan, *supra* note 104, at 461 (stating "state laws can vary in their coverage of cyberharassment because of the way they define conduct and intent sufficient for criminalization in their statutes" and providing examples of states, such as California and Massachusetts, which require showing "repeated attempts of harassment to win a cyberharassment suit" and states, such as Michigan and Arkansas, where only one incident will suffice).

188. *See* TEX. PENAL CODE ANN. § 42.07(a)(7), *declared unconstitutional by* State v. Chen, 615 S.W.3d 376 (Tex. App.—Houston [14th Dist.] 2020, no pet.) (requiring electronic communications be repeated for the action to be considered an offense). Though *Chen* declared this statute unconstitutional, the Texas Legislature is, as of the time of this writing, working on updates to the statute. Every bill still includes the requirement the actions be repeated to be actionable. *See supra* notes 112–114 and accompanying text.

189. *See supra* text accompanying notes 104–09 (analyzing problems arising when electronic communication must be repeated to fall under harassment statutes and providing examples of doxers able to escape prosecution under such statutes).

190. *See* Meritor Sav. Bank v. Vinson, 477 U.S. 57, 67 (1986) ("For sexual harassment to be actionable, it must be sufficiently severe or pervasive 'to alter the conditions of [the victim's] employment and create an abusive working environment.'" (quoting Henson v. Dundee, 682 F.2d 897, 904 (11th Cir. 1982) (alteration in original))).

191. *See* Brian Long, Case Note, *First Amendment Electronic Speech:* Ex Parte Reece*, a Missed Opportunity to Narrow Texas's Unconstitutionally Overbroad Anti-Harassment Statute*, 71 SMU L. REV. 599, 600 (2018) ("The current anti-harassment statute is unconstitutionally overbroad because it includes vague terms [such as 'annoy' and 'alarm'] lacks other limiting language, and potentially extends to non-harassing situations based on prosecutorial discretion.").

"annoy."[192] It may also be necessary to define the word "severe," should it be added to the statute.[193] This may help the statute address individual instances of cyberharassment that expose victims to danger.[194] Texas should specifically proscribe doxing and swatting, including this language in such a statute. If Texas does not create a new statute, the legislature should at least redefine the current harassment statute to encompass both repeated *or* severe electronic communication harassment. This will help protect victims from a greater degree of swatting, doxing, and malicious and dangerous cyberharassment in general.

D. *Instituting Continuing Law Enforcement and Legal Education Are Necessary Steps to Help Victims of Cyberharassment*

In addition to crafting statutes proscribing doxing and swatting, Texas should institute continuing education for law enforcement, lawyers, and judges covering cyberharassment. When victims inform police or judges about cyberharassment, many experience a range of responses from a general dismissal of the threats as jokes[195] to derision.[196] According to Dr. Greg White, director of the Center for Infrastructure Assurance and Security at the University of Texas at San Antonio, and Ms. Julina Macy, who have worked with law enforcement regarding cybersecurity, many in law enforcement do not understand how easy it is to find someone's personal information on the internet.[197] Some neither understand the need for computers nor how much information the younger generations put on the internet and the ways that information may be used against them.[198] When asked how often law enforcement, judges, and lawyers should receive

192. *See id.* at 602 ("[T]he words *alarm* and *annoy* as used in Section 42.07(a)(7) are vague.").

193. Such a definition may help the statute proscribe actions that are "of an extreme degree" to the point "no reasonable person in a civilized society should be expected to endure it." *Severe*, BARRON'S LAW DICTIONARY (7th ed. 2016) (defining "severe" in the context of proving severe emotional distress).

194. *See supra* notes 105–09 and accompanying text (providing examples of doxing and cyberharassment that placed victims in danger).

195. *See* Jason, *supra* note 13 (stating Brianna Wu, during Gamergate, lost "at least a day each week 'explaining the Internet' to the police" and convincing them "Twitter isn't 'just for jokes,' but is in fact her primary means of marketing her business").

196. *See* Marshak, *supra* note 38, at 518 (providing an example of a victim of harassment who stated, after she told the police about threats someone sent from out of state, officers "offered to take down a report, but admitted . . . nothing would come of it unless someone one day put a bullet in [her] brain").

197. White, *supra* note 129.

198. *Id.*

continuing education regarding changes in technology, Dr. White and Ms. Macy stated "it depends," since changes in security follow changes in technology.[199] Therefore, law enforcement and legal associations should institute continuing education for their members, and program organizers should seek professional guidance from those who understand changes in technology and implications these changes have on both security and the law.[200]

Professor Robert Summers of St. Mary's School of Law agrees technology is developing rapidly on all fronts, to the point where it is difficult for the law to keep up.[201] He explains although the reach of technology is difficult to control using traditional jurisdictional theories since it defies jurisdiction as it is currently understood, lawyers must address these issues within existing legal frameworks.[202] When asked about ideas for instituting continuing legal education for law enforcement and the legal community in the area of cyberharassment, Professor Summers suggested collaborating with practitioners and educational institutions, such as law schools and university cybersecurity programs, first to collect input, then to develop a strategy for continuing legal education credits where the instruction may be upgraded when necessary.[203]

As a basis for education, Professor Summers recommends starting with cybertechnology core concepts so participants may understand the technical language before moving on to specific programs focused on doxing and swatting.[204] This approach gives law enforcement, judges, and lawyers who do not understand technology's rapid development, similar to those whom Dr. White and Ms. Macy have worked with,[205] the foundations necessary to understand cyberharassment basics and terminology, thus providing a better understanding of victims' complaints. Further education regarding cyberharassment, doxing, and swatting would help impress upon these professionals the dangers these actions pose. Texas may also consider

199. *Id.*

200. Due to the intricacies of investigating cybercrimes, it may be necessary to train officers to handle complex cyber investigations or involve a cyber specialist in the investigation. Cybercriminals are often well-versed in hiding their identities online and when making swatting calls. Investigators should be prepared and "[e]xpect to encounter proxy servers, virtual private networks, and anonymizing networks." Bernstein, *supra* note 178, at 54.

201. Summers, supra note 185.

202. *Id.*

203. *Id.*

204. *Id.*

205. White, *supra* note 129.

having entities, such as the Texas Bar or a commercial vendor working in continuing education, check with cybersecurity professionals to determine whether to upgrade such instruction.[206] Doing so annually or biannually will help professionals understand the complexities of cybercrimes and keep them apprised of changes. This would help ensure cyberharassment victims are treated fairly and that their situations are handled with the gravity they demand and deserve.

VI. CONCLUSION

Law in the United States has a difficult time keeping up with technology.[207] While there are no federal swatting or doxing laws in the United States,[208] individual states may choose to implement laws regulating the practices, but even where they exist, they are often ineffective or underdeveloped.[209] Though it would be ideal for the United States Congress to develop effective doxing and swatting laws that would uniformly regulate the practices across the nation, it is unlikely any effective laws will be passed on this topic in the near future.[210] Even Congresswoman Kathrine Clark, who became a victim of swatting after she sponsored a bill to criminalize the action, could not convince Congress to pass a law on the subject.[211] For this reason, Texas, a state with experience crafting laws proscribing malicious computer crimes,[212] should work to

206. Summers, *supra* note 185.

207. *Id.*; *see, e.g.*, *Legal Consequences of Swatting*, *supra* note 123 (providing a statement by Professor Neal Katyal of Georgetown University stating "the law hasn't totally caught up to this type of thing" concerning the swatting-related death of Andrew Finch).

208. *See* TEXAS GUIDE, *supra* note 15, at 2 (stating while doxing and swatting are not ethical, the legality of the activities "is not clearly established and varies across jurisdictions").

209. Although California has a swatting law, Professor Neal Katyal points out it may not effectively penalize Andrew Finch's swatters because swatting does not typically result in death. Consequently, the law may not have been constructed in such a way to consider different degrees of swatting. *See Legal Consequences of Swatting*, *supra* note 123 (describing how current swatting laws do not capture the degrees of tragedies that may occur).

210. It is unlikely the federal government will approve any bills regarding doxing or swatting in the near future, as evidenced by the amount of bills on the subject that have died. *See supra* note 53 and accompanying text (providing citations to various U.S. House and Senate bills that died).

211. *See* Calabro, *supra* note 40, at 55 (describing how Congresswoman Kathrine Clark was swatted after police received an anonymous tip there was an active shooter at Clark's house); *Rep. Katherine Clark 'Swatted' After Sponsoring Bill to Criminalize the Hoax*, WBUR (Feb. 4, 2016), https://www.wbur.org/radioboston/2016/02/04/clark-swatting [https://perma.cc/4MYL-RHL8] (indicating swatters attacked Congresswoman Clark after she authored a bill to criminalize the action).

212. *See, e.g.*, Varghese, *supra* note 171 (providing information about "David's Law," which criminalizes cyberbullying in Texas).

proscribe doxing, swatting, and other malicious forms of cyberharassment that may expose victims to physical danger.

Some issues still make crafting such laws difficult. Though doxing and swatting are politicized,[213] supporters on both sides of the aisle participate in and oppose the practice.[214] Generally, Texans seem to understand computer crimes are committed indiscriminately, resulting in David's Law, which criminalized cyberbullying,[215] and House Bill 2789, which criminalized the electronic transmission of sexually explicit material such as sending unwanted nude photographs over text, email, and social media.[216] Another issue making crafting these laws difficult is possible infringement on free speech if found to be vague or overly broad.[217] Basing doxing and swatting laws on existing harassment and other computer crime regulation, however, may help the statute avoid a constitutional challenge.

A few laws useful as a basis for doxing and swatting laws include Texas Penal Code Section 42.07, the Harassment Statute,[218] and Texas Penal Code Section 33.07, the Online Impersonation Statute.[219] Section 42.07

213. *See* Daniel Friend, *Conservatives at UT Austin Unfazed by Doxxing Threats*, TEXAN (July 4, 2019), https://thetexan.news/conservatives-at-ut-austin-unfazed-by-doxxing-threats/ [https://perma.cc/Y2P2-UQAC] (discussing how an incident where a small anarchist group threatened to dox freshman entering the University of Texas at Austin received wide coverage from Fox News and Breitbart and, according to some, was blown out of proportion); *see also* Malone, *supra* note 8 (stating Gamergaters targeting people like Zoë Quinn switched their focus from harassing Gamergate victims to tweeting about "#MAGA" and exploring white nationalism).

214. *See* Callum Borchers, *Doxxed Trump Donors Have an Unlikely Defender in this Democratic Congressional Candidate*, WASH. POST (Apr. 30, 2017, 6:30 AM), https://www.washingtonpost.com/news/the-fix/wp/2017/04/30/doxxed-trump-donors-have-an-unlikely-defender-in-this-democratic-congressional-candidate/ [https://perma.cc/F4XV-KELY] (describing how Brianna Wu, who is a Democrat, a fierce critic of former President Trump, and who launched a 2018 congressional campaign after President Trump was elected, still defended people who donated to the Trump campaign and were, as a result, doxed by an automated Twitter account).

215. *See* Varghese, *supra* note 172.

216. *See* Troy Closson, *A New Texas Law Criminalizes Sending Unwanted Nudes. Lawyers Say It Might Be Difficult to Enforce.*, TEX. TRIB. 1–2 (Aug. 14, 2019, 12:00 AM), https://www.texastribune.org/2019/08/14/Texas-new-law-sending-unwanted-nudes-dating-apps-texts/ [https://perma.cc/9N89-X6FN] (describing how such actions could potentially result in a Class C misdemeanor).

217. This is what happened to the law the Texas Legislature passed criminalizing revenge porn. In April of 2018, a state appeals court declared the law unconstitutional because its broad restrictions infringed on free speech. Legal experts also state House Bill 2789, which criminalizes the electronic transmission of sexually explicit material, may experience legal challenges due to overbreadth and vagueness. *See id.* at 3.

218. TEX. PENAL CODE ANN. § 42.07, *declared unconstitutional by* State v. Chen, 615 S.W.3d 376 (Tex. App.—Houston [14th Dist.] 2020, no pet.).

219. *Id.* at § 33.07.

may serve as a base for criminalizing malicious cyberharassment in general. Section 33.07 creates a base for a doxing statute criminalizing revealing a person's personal information online without their consent when such doxing constitutes a true threat.[220] The Texas Legislature should also consider using a recklessness standard to assess whether something is a true threat, as cyberharassers may escape prosecution under a "purposeful" or "knowing" standard by saying their conduct is just a joke.[221]

Though there is no federal or state law against swatting in Texas,[222] Texas should criminalize the act and look to other states to craft a law considering swatting's different degrees, including death, injury, and peaceful dissolution.[223] Texas should also consider breaking down other cyberharassment laws into degrees, as doxing may also put someone in physical danger.[224]

Additionally, Texas should consider implementing continuing education programs for law enforcement, lawyers, and judges addressing cyberharassment, doxing, and swatting. Technology advances quickly, and as technology changes, so does security.[225] For this reason, Texas should work with practitioners and educational institutions, such as law schools and university cybersecurity programs, to develop programs educating those who will handle these cases.[226] Doing so will help ensure authorities handle malicious cyberharassment with the attention and gravity it requires.

220. *Id.*; *see supra* notes 64, 143, 160 and accompanying text (defining a true threat).

221. *See* Edwards, *supra* note 15 (providing an example of the doxer who, after admitting he realized issuing threats was a federal crime, claimed his rape, bomb, and death threats were a joke, and was able to escape prosecution).

222. *See* TEXAS GUIDE, *supra* note 15, at 2 (noting though swatting and doxing are not ethical, the legality of the practices "is not clearly established and varies across jurisdictions").

223. *See supra* notes 176–80 and accompanying text (discussing the necessity of laws taking into account degrees of swatting).

224. *See* Marshak, *supra* note 38, at 527–28 (describing a particularly frightening threat Brianna Wu received that indicated the doxing and harassment she experienced exposed her to danger).

225. White, *supra* note 129.

226. Summers, *supra* note 185.