

FROM VIRTUAL TO VIOLENCE: EVOLVING TORT LIABILITY TO COMBAT DOXXING & SWATTING

Morgan N. Murphy-Sterger*

INTRODUCTION

Imagine this: It is a chilly December evening, just three days after Christmas. You are relaxing on your living room couch, scrolling through your phone, enjoying the comfort and safety of your own home. It is a quiet evening as your mother, niece, and other relatives who live with you are relaxing in their bedrooms. You hear a noise outside and, assuming it's the kids' friends coming to visit, you open the front door. For Andrew Finch of Wichita, Kansas, this was the last time he would open his front door. Outside Andrew's home on the night of December 28, 2017, there were dozens of police SWAT team officers, blinding spotlights, and the confusion of dozens of officer's voices yelling at him. Amidst the confusion, Andrew dropped his hands and was fatally shot by a sniper rifle on his porch.¹ Andrew Finch was the victim of a cruel and senseless "prank" called swatting that began as a disagreement over a video game.

Swatting hoaxes are significantly increasing in frequency and can happen to anyone. In 2020, a grandfather, Mark Herring, died of a heart attack in a swatting incident after being harassed online by individuals who wanted his unique Twitter username.² Politicians such as Representative Katherine Clark and New Jersey Assemblyman Paul Moriarty were both swatted after introducing anti-swatting legislation.³ In 2022, there were four swatting incidents against Twitch streamers in one week, which is a confounding amount that speaks to seriousness of this growing epidemic of pervasive online harm.⁴ Many people, ranging from politi-

* J.D. Candidate, The University of Toledo College of Law (May 2025). I want to express my gratitude to my faculty advisor, Dean Geoffrey Rapp, for his guidance on this paper, as well as my family and friends for their support during this year. A very special thanks to my husband, Nick, and my son, William, for being my rocks and providing me with their unwavering love and support.

1. Brendan I. Koerner, *It Started as an Online Gaming Prank. Then It Turned Deadly*, WIRED (Oct. 23, 2018, 6:00 AM), <https://www.wired.com/story/swatting-deadly-online-gaming-prank/>.

2. Maria Cramer, *A Grandfather Died in 'Swatting' Over His Twitter Handle, Officials Say*, N.Y. TIMES (July 24, 2021), <https://www.nytimes.com/2021/07/24/us/mark-herring-swatting-tennessee.html>.

3. Ryan Grenoble, *'Swatting' Is Endangering Lives, Aided in Part by a Legal Loophole*, HUFFPOST (June 7, 2018, 3:59 PM), [https://www.huffpost.com/entry/deadly-prank-endangering-lives_n_5b17fca6e4b09578259e132b?re8=](https://www.huffpost.com/entry/deadly-prank-endangering-lives_n_5b17fca6e4b09578259e132b?re8=;); Elizabeth M. Jaffe, *Swatting: The New Cyberbullying Front After Elonis v. United States*, 64 DRAKE L. REV. 455, 468 (2016).

4. Nathan Grayson, *Twitch Streamers Traumatized After Four 'Swattings' in a Week*, WASH. POST (Aug. 15, 2022, 1:34 PM), <https://www.washingtonpost.com/video-games/2022/08/15/keffals-adin-ross-ishowspeed-swatting-twitch-youtube/>.

cians to celebrities to activists to video game streamers, have found themselves to be the victims of a swatting hoax either in retaliation for their views or activities or to harm or embarrass the swatting victim. Even more people have been victims of another form of online harassment called doxxing (also sometimes spelled doxing), in which the victim's personal information is published in an online forum, opening them up to further harassment.⁵ Doxxing harassment usually precedes and leads to a swatting incident. These interconnected forms of online harassment can cause injuries to victims including emotional distress, physical injury, and monetary damages. And although current tort frameworks may provide remedy to victims, they should be enhanced to encompass swatting and doxxing.

New developments in the law surrounding doxxing and swatting include newly recognized online harassment torts in Washington State and Ontario, Canada, as well as a new anti-doxxing statute in Oregon. In Washington State, the new common law tort is the result of repeated online harassment and the doxxing of a video game developer's employees and the Ontario common law tort came after a defendant carried out "'systemic campaigns of malicious falsehood' by making anonymous and pseudonymous posts" on social media platforms towards the victim.⁶ The Oregon statute, enacted in 2021, gives victims of doxxing a cause of action for having their personal information posted or uploaded online.⁷ These new laws can significantly help deter, and provide remedies for doxxing and swatting harassment, and other jurisdictions should consider adopting these new laws.

Swatting and doxxing are becoming prevalent in today's increasingly online world and have affirmatively caused serious tortious harm to victims of these behaviors. Although there is legal recourse for swatting and doxxing on the criminal side of the law, there is a dire need for civil causes of action specifically aimed at targeting these types of harassing behaviors. This Comment examines the aspects of doxxing and swatting and analyzes the effectiveness of current tort law in remedying these harms. This Comment argues current tort frameworks are inadequate on their own to provide a complete remedy for victims of and to deter swatting and doxxing, and recommends jurisdictions recognize new tort causes of action tailored to address online harassment in the form of swatting and doxxing.

I. BACKGROUND ON SWATTING & DOXXING AS FORMS OF ONLINE HARASSMENT

The anonymity of the internet has created a host of online harassment, in which perpetrators of this harassment are rarely held accountable for their heinous

5. Kristi S. Schubert, *A Cousin to Identity Theft, 'Doxxing' Is on the Rise*, LA. ADVOCS., Apr. 2015, at 13, 13.

6. Paul Tassi, *'Destiny 2' Player Who Terrorized Bungie Community Manager Must Pay Almost \$500,000*, FORBES, <https://www.forbes.com/sites/paultassi/2023/07/13/destiny-2-player-who-terrorized-bungie-community-manager-must-pay-almost-500000/?sh=2162a4905bbe> (July 14, 2023, 4:38 PM); Jessica Warwick & Heather Cameron, *Ontario Superior Court Recognizes New Tort of Internet Harassment*, NORTON ROSE FULBRIGHT (Feb. 12, 2012), <https://www.nortonrosefulbright.com/en-ca/knowledge/publications/8b2cfc45/ontario-superior-court-recognizes-new-tort-of-internet-harassment>.

7. OR. REV. STAT. ANN. § 30.835(2) (2021).

conduct. Doxxing and swatting are two forms of online harassment that invade an individual's privacy and have affirmatively caused severe emotional and physical harm to its victims. But it is difficult for these victims to pursue civil legal remedies. Doxxing and swatting are interrelated forms of harassment because, in many cases, a dox occurs and gives the address and information needed to conduct the swatting. Swatting can be considered "[a] [d]angerous [o]ffshoot of [d]oxxing" because in many cases "a swatter uses personal information obtained through a dox... to place a distress call or target the victim at that address."⁸ Doxxing and swatting are also both very prevalent in, and are commonly used as an outlet for toxicity within, the online gaming community. Bad actors within the online video game world use doxxing and swatting as tools to harass video game streamers due to gender, race, religion, and other factors. It is also used as a method of bullying, harassment, or retribution against opposing players in competitive games.

Doxxing and swatting are both punishable under various criminal statutes. These include federal laws prohibiting false information and hoaxes, stalking laws, or wire fraud for relaying false information via wire communication leading to a waste of police resources.⁹ Many states have statutes making it illegal to call in false threats or emergencies. Some state statutes make calling in a false threat a hate crime if it is "racially motivated or stem[s] from other prejudices against protected groups."¹⁰ Additionally, a few states, such as Ohio and Oregon, have enacted criminal statutes specifically outlawing swatting or doxxing.¹¹ Although these criminal laws are helpful in combating swatting and doxxing, they cannot provide a remedy to victims to fully compensate them for injuries and damages sustained. Thus, tort causes of action specifically aimed at swatting and doxxing conduct are needed to provide additional deterrence and to compensate victims for their injuries.

A. Doxxing Defined

"Doxxing—named for 'documents' or 'docs'—is the act of releasing someone's personal and/or identifiable information without their consent."¹² This personal information can include their real name, home or work addresses, photographs, financial information, phone numbers, and information about their

8. Victoria McIntyre, "Do(x) You Really Want to Hurt Me?": *Adapting IIED as a Solution to Doxing by Reshaping Intent*, 19 TUL. J. TECH. & INTELL. PROP. 111, 115 (2016) (citing Alex Hern, *Gamergate Hits New Low with Attempts to Send Swat Teams to Critics*, GUARDIAN (Jan. 13, 2015, 9:57 AM), <https://www.theguardian.com/technology/2015/jan/13/gamergate-hits-new-low-with-attempts-to-send-swat-teams-to-critics>).

9. Kelly Martin, *The Crime of Swatting: Laws and Penalties*, NOLO, <https://www.nolo.com/legal-encyclopedia/the-crime-of-swatting-laws-and-penalties.html> (Dec. 16, 2022).

10. *Id.*

11. Ashley Silver, 'Swatting' Now a Felony Under Ohio Governor's New Law, POLICE1 (Jan. 4, 2023, 11:51 AM), <https://www.police1.com/legal/articles/swatting-now-a-felony-under-ohio-governors-new-law-7WgkegICV0SQoexk/>; OR. REV. STAT. ANN. § 30.835 (2021).

12. Andrew Quodling, *Doxxing, Swatting, and the New Trends in Online Harassment*, THE CONVERSATION (Apr. 21, 2015, 4:11 PM), <https://theconversation.com/doxxing-swatting-and-the-new-trends-in-online-harassment-40234>.

family.¹³ Doxxing can be defined as “the public release of an individual’s private, sensitive, personal information, such as [their] [h]ome address, [e]mail address, [p]hone number, [s]ocial security number, [e]mployer and employer contact info[rmation], [f]amily member’s contact info[rmation], [and p]hotos of victim’s children and the school they attend.”¹⁴ Many forums that people dox on are for the purpose of inciting violence or harassment.¹⁵ Perpetrators often dox an individual to encourage others to harass the victim. This can lead to swatting.¹⁶ Doxxing accomplishes two things for online harassers: (1) it invades the victim’s privacy, which can intimidate the victim, and (2) it gives potential harassers the resources they need to torment the victim in the future.¹⁷ Doxxing is an effective method of harassment because the internet is very public, instantaneous, and allows for harassment on an enormous scale. Perpetrators of online harassment often use doxxing in conjunction with swatting. In many instances, multiple perpetrators are involved in the campaign of harassment aimed at the victim.¹⁸

Doxxing someone puts them in danger of facing phone harassment, credit card fraud, and more.¹⁹ Doxxing also allows the victim’s personal information to become even more accessible on the internet and opens victims up to the potential for further harassment or physical real-world violence in the form of stalking or swatting.²⁰ Doxxers can gain their information from online searches, fake phone calls to utility companies, and various other public sources or fraudulent methods.²¹ Doxxing can often escalate to real-world physical violence and lead to the victim being swatted.

B. Swatting Defined

“Swatting” is a dangerous form of online harassment that involves a perpetrator making a 911 call and reporting a false crime at the swatting victim’s address with the intention of inducing a police special weapons and tactics (“SWAT”) team response.²² Usually, the swatter reports that a horrific crime, such as a killing or taking of hostages, has taken place at the target’s address when no such crime has occurred.²³ Perpetrators of swatting hoaxes can get their victim’s personal informa-

13. *Id.*; Schubert, *supra* note 5.

14. Julia M. MacAllister, *The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information*, 85 FORDHAM L. REV. 2451, 2456 (2017) (quoting Mary Anne Franks, Professor, Univ. of Miami Sch. Of Law, Remarks at the American Bar Association Program on Doxing, Swatting, Trolls, and SJWs: Harassment and Gender Discrimination on Social Media Platforms (Nov. 8, 2016) (on file with the Fordham Law Review)).

15. Schubert, *supra* note 5.

16. *Id.*

17. Quodling, *supra* note 12.

18. MacAllister, *supra* note 14.

19. Jason Fagone, *The Serial Swatter*, N.Y. TIMES MAG. (Nov. 24, 2015), <https://www.nytimes.com/2015/11/29/magazine/the-serial-swatter.html>.

20. MacAllister, *supra* note 14, at 2457.

21. Quodling, *supra* note 12.

22. *Id.*

23. Jaffe, *supra* note 3, at 456.

tion such as addresses or phone numbers that they use to harass the victim via doxxing. The perpetrators use modern technology to mask their voice, their phone number, and their location or IP address.²⁴ These actors abuse the crime reporting system to torment and harm their victim. “[S]watting hoax[es] [are] often preceded by other kinds of Internet attacks,” such as social media threats or doxxing.²⁵ Swatting is an escalation of doxxing and other internet harassment and is the most dangerous because the harassment is no longer virtual but becomes real world and physical via the actual weapons and confusion involved.²⁶

Swatting hoaxes have been around for decades, starting in the mid-2000s, but have significantly increased in frequency with the rise of livestreaming on websites such as Twitch or YouTube.²⁷ Swatting incidents often happen to popular video game streamers, celebrities, politicians, activists, and even schools. “By 2019, there were an estimated 1,000 swatting incidents in the U.S. each year... and each incident is estimated to cost at least \$10,000 to affected communities...”²⁸ The victims themselves also incur monetary, physical, and emotional injuries that cannot be adequately remedied by criminal legal action alone.

C. *Victims of Swatting*

Both methods of online harassment have been used to harm and harass many people and have been a popular harassment technique used in the gaming world. One of the most notorious and shocking cases of swatting took place in 2017 and involved a dispute over the video game, *Call of Duty*.²⁹ There, two gamers, Casey Viner of Ohio and Shane Gaskill of Kansas, got into an argument while playing *Call of Duty*. Viner then contacted Tyler Barriss (a prolific swatter) to swat Gaskill, and Gaskill “dared” Barriss to swat him, giving him a Wichita, Kansas, address that Gaskill formerly resided at.³⁰ Barriss then swatted the address, and the house’s current resident, Andrew Finch, was killed by the responding police when an officer thought he saw Finch reach for a weapon.³¹

Many other instances of swatting happened in the video game community. In 2014, Jordan Mathewson was streaming the game *Counter-Strike* live to viewers when he was swatted. Police raided his home while he was live broadcasting his

24. Jacob Ward & Lora Kolodny, *The FBI Has Formed a National Database to Track and Prevent ‘Swatting’*, NBC NEWS (June 29, 2023, 6:40 PM), <https://www.nbcnews.com/news/us-news/fbi-formed-national-database-track-prevent-swatting-rcna91722>.

25. Fagone, *supra* note 19.

26. *Id.*

27. Emma Witman, *What Is Swatting? The Act of Making False Police Reports with Malicious Intent and How to Protect Yourself from It*, BUS. INSIDER (Jan. 5, 2021, 4:32 PM), <https://www.businessinsider.com/guides/tech/what-is-swatting>.

28. Ward & Kolodny, *supra* note 24.

29. Brice-Saddler et al., *Prankster Sentenced to 20 years for Fake 911 Call That Led Police to Kill an Innocent Man*, WASH. POST (March 29, 2019), <https://www.washingtonpost.com/nation/2019/03/29/prankster-sentenced-years-fake-call-that-led-police-kill-an-innocent-man/>.

30. *Id.*

31. *Id.*

video game and arrested him in front of his viewers.³² In 2019, a sixteen-year-old *Fortnite* streamer, Kyle Giersdorf, was also swatted while broadcasting live. But in that case, an officer recognized Kyle and realized it was a hoax.³³ In 2022, four popular streamers on the website Twitch were swatted in one week.³⁴ Those streamers described the experience as “[t]raumatizing and an invasion of their privacy due to the extreme confusion and fear that is caused by police officers suddenly bursting into their homes with weapons drawn.”³⁵ One prolific swatter, known as Obnoxious, harassed multiple women who streamed on Twitch by doxxing and swatting them in what would become “part of one of the most disturbing crime sprees in Internet history.”³⁶

Gamers are not the only ones who can become victims of doxxing or swatting. Politicians and activists have also been swatted for introducing anti-swatting legislation or for speaking out on a hot button issue. In 2016, Representative Katherine Clark was swatted in her home after introducing her Interstate Swatting Hoax Act of 2015, and in 2019, a swatting incident was committed against Black Lives Matter activist, Melina Abdullah.³⁷ Many celebrities have also found themselves at the receiving end of a swatting prank such as Tom Cruise, Miley Cyrus, Justin Bieber, and many others. Author Patrick Tomlinson and his wife, Niki Robinson, have been the victims of swatting more than forty times at their home in Milwaukee, suffering emotional injury and physical damages to their home each time.³⁸ Over the course of one week in April 2023, “universities including Clemson, Florida, Boston, Harvard, Cornell, Pittsburgh, Rutgers and Oklahoma, as well as Middlebury College, were targeted by swatters.”³⁹ Anyone can find themselves a victim of a dox or swatting for the most mundane reasons such as a feud over a video game, a difference in opinions in an online forum, or even for having a unique username on social media. Simply having a public presence can put someone at risk of being swatted or doxxed, but a public presence is not required for someone to be victimized.

Doxxing is even more prevalent than swatting and can happen to everyone, not just those who have a platform. Georgia election workers in 2022 became victims of doxxing after Rudy Giuliani went on a media campaign accusing them of election fraud.⁴⁰ The election workers, singled out by Giuliani, became victims of harassment after their information was doxxed online. They had strangers camped out outside their homes, malicious Christmas cards mailed to their homes containing threatening messages, received threatening phone calls, had pizza

32. Witman, *supra* note 27.

33. *Id.*

34. Grayson, *supra* note 4.

35. *Id.*

36. Fagone, *supra* note 19.

37. Grenoble, *supra* note 3; Witman, *supra* note 27.

38. Ward & Kolodny, *supra* note 24.

39. *Id.*

40. Freeman v. Giuliani, 2022 WL 16551323, at *4 (D.D.C. 2022).

deliveries ordered to their homes, and had to change phone numbers and emails because of the flood of harassment caused by doxxing.⁴¹

Doxxing and swatting can cause significant injury to victims in the form of physical injury, emotional distress, loss of earnings, and damage to their home or property. These forms of online harassment can happen to anyone and for many mundane reasons. Swatting and doxxing are serious issues that are drastically increasing in frequency and the level of danger involved. Current tort law may provide some remedy to victims of these types of online harassment but does not fully address the specific aspects of online harassment in these forms.

II. CURRENT TORT REMEDIES AVAILABLE TO VICTIMS OF SWATTING & DOXXING

A. *Intentional Infliction of Emotional Distress (“IIED”)*

Current tort law provides a few options for victims to redress their injuries caused by doxxing and swatting. One such tort cause of action available to victims is intentional infliction of emotional distress (“IIED”). The Second Restatement of Torts defines IIED as “[o]ne who by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another is subject to liability for such emotional distress....”⁴² IIED can be a civil cause of action for victims of swatting or doxxing because the consequences of a swat or dox can be significantly distressing and outrageous. Some issues that may be encountered when pursuing an IIED claim in swatting and doxxing cases include First Amendment protections and establishing that a pattern of conduct can be outrageous and extreme.

In one case of doxxing, *Freeman v. Giuliani*, election workers were the victims of online harassment in which they were accused of election fraud online and followers of the defendant were encouraged to harass the victims.⁴³ The victims’ personal information was found online and used by people to further harass them by camping outside of, sending threatening letters to, and pizza orders being delivered to their homes.⁴⁴ Additionally, the victims in this case received threatening calls to their own and their family members’ phones, threatening and harassing messages on their social media pages, and strangers camping outside of and harassing them at their workplaces as a result of the dox.⁴⁵ The court there allowed the plaintiff’s claim for IIED resulting from the defendant’s harassment of and encouragement of others to harass the plaintiffs.⁴⁶ The defendant in *Freeman* acted in an extreme and outrageous manner when he accused these election workers of fraud continuously, even after the fraud was proven to not have taken place, and his conduct of encouraging others to harass the victims could also be seen as outrageous or extreme to the reasonable person. This conduct was

41. *Id.*

42. RESTATEMENT (SECOND) OF TORTS § 46 (AM. L. INST. 1965).

43. *Freeman*, 2022 WL 16551323, at *4.

44. *Id.*

45. *Id.*

46. *Id.* at *10.

intentional and caused these victims to suffer significant emotional distress because the victims were left “feeling fearful,” were afraid to go to work or go in public, lost friendships, and one victim even ceased operation of her online business.⁴⁷

In some cases, doxxing and the harassment that follows from it can lead to the more dangerous hoax of swatting. Swatting also can create a cause of action for IIED because the perpetrators intentionally call in a fake emergency to provoke a police response to their victim’s address. Victims of swatting suffer severe emotional distress due to having heavily armed police officers entering their home when they have not committed any crime. In one case of swatting, a woman was awoken in the middle of night to police officers with weapons drawn in her living room.⁴⁸ Another person, who was swatted while streaming live on Twitch, described the experience of being swatted as “[t]raumatizing.”⁴⁹ Harassment in the form of doxxing and swatting can constitute outrageous conduct resulting in severe emotional distress to the victims.

Harassment from doxxing and swatting may not be just one isolated emotionally distressing incident but often may take place continuously over a period of time. In *Bustamento v. Tucker*, the court explained how not every encounter or action can be converted into a tort and that, to recover for IIED, the conduct must be outrageous and so extreme “as to go beyond all possible bounds of decency and be regarded as atrocious and utterly intolerable in a civilized community.”⁵⁰ In this case, a pattern of sexual harassment in a workplace took place over the course of two years.⁵¹ The harassment took place almost daily and on many occasions the harassment reduced the victim to tears and left her emotionally distraught.⁵² The harassment in *Bustamento* consisted of verbal threats, degrading statements, and physical conduct. There, the court noted “both the intensity and the duration of the distress are factors to be considered in determining whether a pattern of conduct is actionable.”⁵³ The court further explained what seems like “‘mild’ harassment may become tortious if continued over a substantial time.”⁵⁴ In cases of swatting and doxxing, each instance on its own may seem like mild harassment not constituting intentional infliction of emotional distress; however, the culmination of the acts of harassment via doxxing or swatting over time can “transform[] the individual incidents of harassment into an actionable tort.”⁵⁵

In one case of extreme doxxing and swatting against several female Twitch streamers, the harassing conduct began in 2013 with harassing threats and doxxing of the women’s personal information by a person known by the username Obnox-

47. *Id.* at *4.

48. Fagone, *supra* note 19.

49. Grayson, *supra* note 4.

50. *Bustamento v. Tucker*, 607 So. 2d 532, 537 (La. 1992) (quoting *White v. Monsanto Co.*, 585 So. 2d 1205, 1209 (La. 1991)).

51. *Id.* at 534.

52. *Id.*

53. *Id.* at 538 (citing RESTATEMENT (SECOND) OF TORTS § 46 cmt. j (AM. L. INST. 1965)).

54. *Id.* (quoting Alice Montgomery, *Sexual Harassment in the Workplace: A Practitioner’s Guide to Tort Actions*, 10 GOLDEN GATE U. L. REV. 879, 890 (1980)).

55. *Id.* at 540.

ious.⁵⁶ Obnoxious was able to find out several women's phone numbers, addresses, IP addresses, and other personal identifiable information by duping customer service representatives of internet companies over the phone.⁵⁷ His harassment of these women escalated into him doxxing them by posting intimate photos of the women, sending pizza deliveries to their homes, and he began swatting the women.⁵⁸ Obnoxious harassed many of these women for over a year, posting their personal information, posting photos of them, and swatting many of them, some multiple times.⁵⁹ This clear and established pattern of continued harassment over time can give rise to tort liability under IIED. Many cases of swatting and doxxing are comparable to Obnoxious's case because the harassment is not one isolated incident but a series of harassing events over a course of time.

In one case, *Gersh v. Anglin*, the defendant argued the IIED damages claimed by the plaintiff were not a reasonably foreseeable consequence of the defendant's actions.⁶⁰ There, the defendant, Anglin, operated an alt-right website with pro-Nazi themes.⁶¹ Anglin published an article to his website, calling for his readers to initiate a "troll storm" upon the plaintiff Gersh.⁶² Within the article, he criticized Gersh's actions, described Gersh using heavy anti-Semitic stereotypes, and called for "confrontation" and "action" against Gersh.⁶³ Anglin doxxed Gersh by publishing in the article "Gersh's phone numbers, email addresses, and social media profiles, as well as those of her husband, twelve-year-old son, friends, and colleagues," encouraging his readers to use the doxxed information to harass Gersh.⁶⁴ Gersh and her family received an onslaught of vicious harassment from readers of Anglin's article, including over "700 disparaging and/or threatening messages over phone calls, voicemails, text messages, emails, letters, social media comments, and Christmas cards."⁶⁵ Gersh filed suit against Anglin with claims of IIED, intrusion upon seclusion, and other causes of action.

Anglin argued the IIED claim was inadequate because he could not have reasonably foreseen the damages caused by his readers as a consequence of the act of doxxing Gersh.⁶⁶ The lower court held Gersh presented an adequate claim for IIED by "alleg[ing] that Anglin assisted, encouraged, and ratified a vicious campaign of anti-Semitic harassment against her and her family."⁶⁷ Thus, the court established the campaign of harassment by Anglin's readers was a reasonably foreseeable consequence of Anglin's act of doxxing Gersh.

Difficulties in imposing liability under IIED arises in the context of First Amendment protections. In *Snyder v. Phelps*, the defendant used the First Amend-

56. Fagone, *supra* note 19.

57. *Id.*

58. *Id.*

59. *Id.*

60. *Gersh v. Anglin*, 353 F. Supp. 3d 958, 970 (2018).

61. *Id.* at 962.

62. *Id.*

63. *Id.* at 963.

64. *Id.* at 962.

65. *Id.* at 963.

66. *Id.* at 970.

67. *Id.*

ment's freedom of speech clause as a defense to a claim of IIED.⁶⁸ In *Snyder*, members of the Westboro Baptist Church picketed a military funeral to communicate their views on homosexuality.⁶⁹ The Court in *Snyder* held the First Amendment was a complete defense to the IIED claim because the conduct involved was a matter of public concern and conducted in a public place.⁷⁰ Conversely, in *Holloway v. American Media, Inc.*, the court held speech is not protected if the only purpose of the speech is to attack a person over a private matter.⁷¹ There, American Media and the National Enquirer published multiple articles and statements deemed to be false regarding the disappearance of Natalee Holloway.⁷² Natalee Holloway's mother sued under IIED. The defendants here, citing *Snyder v. Phelps*, argued "the First Amendment provid[ed] a bar to state-law tort claims."⁷³ The Court there rejected this argument, stating "the First Amendment protection described in *Snyder* does not extend to speech... that is used as a weapon simply to mount a personal attack against someone over a private matter."⁷⁴

Instances of doxxing and swatting that are purely malicious in nature, and not politically motivated, are like that of the *Holloway* case as opposed to the *Snyder* case. Doxxing peoples' personal information to harass them and encourage harassment by others is not a public matter or of legitimate public concern. Doxxing someone could reasonably be interpreted as being speech that is "used as a weapon simply to mount a personal attack" against the victim over a private matter.⁷⁵ Additionally, there are likely no First Amendment protections for those who commit swatting because swatting is conduct, and conduct is not speech protected by the First Amendment.⁷⁶ The conduct standard from *United States v. O'Brien* could also arguably apply to instances of doxxing because doxxing someone with the intent to harass is also conduct, not speech within the meaning of the First Amendment. "While speech and expression may not be easily restrained, the manipulative and unauthorized use of others' data and the deception of police forces can be prevented" as these actions constitute conduct which is not afforded First Amendment protection.⁷⁷ Thus, First Amendment limitations to IIED would likely not apply in cases of doxxing and swatting when committed for purely malicious purposes, making IIED a viable tort remedy for victims doxxing and swatting.

68. *Snyder v. Phelps*, 562 U.S. 443, 451 (2011).

69. *Id.* at 448.

70. *Id.* at 456.

71. *Holloway v. Am. Media, Inc.*, 947 F. Supp. 2d 1252, 1269 (N.D. Ala. 2013).

72. *Id.* at 1258.

73. *Id.* at 1261 (citing *Snyder*, 562 U.S. at 460-61).

74. *Id.* at 1262.

75. *Id.*

76. *United States v. O'Brien*, 391 U.S. 367, 376 (1968).

77. Lisa Bei Li, *Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting*, 70 FED. COMM. L.J. 317, 319 (2018); see also *O'Brien*, 391 U.S. at 376-77.

B. Invasion of Privacy

Additionally, tort causes of action for invasion of privacy may provide victims of doxxing or swatting with a remedy for their injuries. The right to privacy was first discussed in the dissent of Justice Brandeis in the 1928 case, *Olmstead v. United States*.⁷⁸ Justice Brandeis defined the right to privacy as “the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.”⁷⁹ The two invasion of privacy torts that would likely be applicable to the conduct of doxxing and swatting are: (1) intrusion upon seclusion, and (2) public disclosure of private facts. Difficulties arise here when a dox is politically motivated, done to a person in the public eye, or when doxxed information is available publicly online. However, invasion of privacy torts can be a viable option. This section discusses swatting and doxxing committed for purely malicious purposes only and not for politically motivated reasons.

1. Public Disclosure of Private Facts

In addition to intrusion upon seclusion, public disclosure of private facts is a cause of action available to victims of doxxing. The Second Restatement of Torts puts it this way:

One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that[:] (a) would be highly offensive to a reasonable person; and (b) is not of legitimate concern to the public.⁸⁰

A matter is publicized when it is “made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge.”⁸¹ If the information is already public knowledge, there is no liability under this tort.

Typically, the information posted online in a dox can include the victim’s phone number, home address, work address, social security numbers, and other personal private information.⁸² This information can constitute private facts for a public disclosure of private facts tort claim. In the case, *Benz v. Washington Newspaper Publishing Co., LLC*, the defendant retaliated against the plaintiff for rejecting his romantic advances by creating fake website dating profiles of her.⁸³ The defendant had posted plaintiff’s home and work phone numbers and addresses on the website pretending to be the plaintiff and stating she was “seeking sexual

78. *Olmstead v. United States*, 277 U.S. 438, 478 (1928).

79. *Id.* at 479.

80. RESTATEMENT (SECOND) OF TORTS § 652D (AM. L. INST. 1977).

81. *Id.* § 652D cmt. a.

82. Margaret Lundeen, *Online Bullying May Alter the Future of the First Amendment*, UIC L. REV. (June 25, 2017), <https://lawreview.law.uic.edu/news-stories/online-bullying-may-alter-the-future-of-the-first-amendment/>.

83. *Benz v. Wash. Newspaper Publ’g Co., LLC*, 2006 WL 2844896, at *1 (D.D.C. 2006).

relations.”⁸⁴ The defendant argued that since the information he posted was already available on the internet, he could not be held liable for disclosing the information.⁸⁵ The *Benz* court held “[a]lthough plaintiff’s phone numbers and addresses may be available to the public on the internet and in phone books, that does not negate the fact that the information are nonetheless private facts,” and thus recognized a privacy interest in phone numbers and home addresses.⁸⁶ Doxxing certain types of private personal information, such as social security numbers, can open a doxxing perpetrator up to criminal liability as well.⁸⁷

In doxxing and swatting cases, the release of phone numbers and addresses poses a significant threat to the victims. The publishing of their personal identifiable information on online forums opens doxxing victims up to physical harassment in the form of swatting, stalking, and other activities that could damage their property, quality of life, and injure them physically and emotionally. Doxxing someone’s private information, of which the public has no legitimate concern, with the goal of furthering the harassment of that person, is conduct that is highly offensive to the reasonable person.

2. *Intrusion Upon Seclusion*

Intrusion upon seclusion is a privacy tort that may provide a remedy to victims of doxxing and swatting. A person may be liable for intrusion upon seclusion if they “intentionally intrude[], physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns... if the intrusion would be highly offensive to a reasonable person.”⁸⁸ Victims of doxxing and swatting have a cognizable right to privacy in information such as phone numbers and addresses, even if that information is available to the public on the internet.⁸⁹ A person need not intrude themselves; they may still be liable for intrusion upon seclusion for negligently permitting a third party to intrude into another person’s affairs.⁹⁰

In *LeCrone v. Ohio Bell*, the defendant installed an extension on the plaintiff’s telephone line at the request of plaintiff’s ex-husband without plaintiff’s knowledge.⁹¹ The plaintiff, unaware of the extension of the line, complained of hearing noises on her phone, “like someone was listening in.”⁹² Later, plaintiff learned of the extension and informed defendant that she never asked for such extension, and it was disconnected the next day. In this case, the defendants argued that since no act of physical trespass occurred and no eavesdropping by their employees or agents occurred, then they had not committed any invasion of

84. *Id.*

85. *Id.* at *7.

86. *Id.* at *8.

87. *See* *United States v. Sutcliffe*, 505 F.3d 944, 960 (9th Cir. 2007).

88. RESTATEMENT (SECOND) OF TORTS § 652B (AM. L. INST. 1977).

89. *Benz v. Wash. Newspaper Publ’g Co., LLC*, 2006 WL 2844896, at *8 (D.D.C. 2006).

90. *LeCrone v. Ohio Bell Tel. Co.*, 201 N.E.2d 533, 538 (Ohio Ct. App. 1963).

91. *Id.* at 536.

92. *Id.*

plaintiff's privacy.⁹³ The court discussed, "defendant 'intentionally' by such means, did allow persons unauthorized by the plaintiff to listen to and intercept plaintiff's private telephone conversations."⁹⁴ The court further explained that "[o]ne who materially aids or abets a wrongful act by another may be as responsible as the one who commits the act, so as to impose liability upon the former to the same extent as if he had performed the act himself."⁹⁵ Defendants could still be held liable in *LeCrone* because, "[f]or harm done to a third person from the tortious conduct of another, a person is liable if he permits the other to act with his instrumentalities knowing or having reason to know that the other is acting or will act tortiously."⁹⁶ The defendants there installed the extension onto plaintiff's telephone line, permitting her ex-husband to listen to her private conversations, and a reasonable person could find this intrusion to be offensive. The *LeCrone* case is comparable to situations of doxxing and swatting for several reasons. When a person doxes another person, they upload the victim's personal information for others to use it to harass the victim.

LeCrone is also comparable to swatting cases because in a swat, a perpetrator calls in a fake emergency knowing a police response will occur at the victim's home. People who swat are permitting a third party to intrude upon the seclusion of another by permitting SWAT officers to storm into the victim's home. Any reasonable person would likely find it highly offensive for a heavily armed SWAT team to intrude upon their seclusion.

C. *Difficulties in Imposing Liability Against Those Who Commit Doxxing or Swatting*

Imposing liability for doxxing and swatting can also be difficult due to the anonymity of the internet and liability exceptions for web service providers whose websites provide the place for doxxers to upload victims' information. Perpetrators of online harm often used tactics to mask their identity by hiding their IP address using proxy servers, VPNs, or by using public Wi-Fi.⁹⁷ In swatting cases, the callers can mask their identity and location by using voiceover internet protocol ("VoIP") to change their phone number to appear to be in the same area code as the victim's.⁹⁸ Swatting perpetrators can also use tactics such as spoofing services to "hide their actual location, change their voice, and insert background noise," as well as creating anonymous profiles on messaging applications or online phone services to "hoax text message and make emergency calls."⁹⁹

93. *Id.*

94. *Id.* at 538.

95. *Id.* (citing *Kuhn v. Bader*, 101 N.E.2d 322, 327-29 (Ohio Ct. App. 1951)).

96. *Id.*

97. Schubert, *supra* note 5, at 19.

98. Ferdinand G. Suba Jr., *The Hoax and the Home: Assessing the Legal Remedies Against Swatting*, ISSUE SPOTTER: CORNELL J.L. & PUB. POL'Y (Nov. 8, 2018), <http://jlpp.org/blogzine/the-hoax-and-the-home-assessing-the-legal-remedies-against-swatting/>.

99. *Id.*

Website service providers hosting doxxed information are usually able to ascertain the perpetrators' identity but often refuse to reveal those identities to protect their financial interests.¹⁰⁰ "Other websites make a conscious effort not to obtain or retain their users' identifying information."¹⁰¹ Additionally, if victims wish to sue the website service providers directly for allowing the personal information to be published on their websites, they often fail due to broad liability defenses provided by Section 230 of the Communications Decency Act of 1996.¹⁰² Section 230 provides: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."¹⁰³ "Section 230 shields website owners and ISPs from liability whenever they act as a 'service provider' and only passively display 'user-generated content'...."¹⁰⁴ However, Section 230 defenses are limited if the website acts in a way that suggests it is a "content provider" as well as a "service provider."¹⁰⁵

These difficulties pose several challenges for victims seeking remedy against perpetrators and the websites enabling the harassment to take place under current tort law. Newer developments in the law surrounding online harassment in a few jurisdictions have the potential to alleviate some of these challenges.

III. A STEP TOWARDS THE FUTURE: NEW TORT CAUSES OF ACTION AIMED AT SWATTING & DOXXING

A. *New Developments in Tort Law*

Washington State and Oregon have recognized new civil causes of action specific to online harassment. Tort law in other countries has also developed to address online harms, with Ontario, Canada recognizing a new online harassment tort. New torts will assist in deterrence of doxxing and swatting conduct and help provide additional remedies to victims of such conduct. The new torts discussed in this section are specifically adapted towards addressing the growing problem of online harassment in the form of swatting and doxxing.

1. *Washington State's New Tort in Response to Bungie, Inc. v. Comer*

The new Washington tort arises out of a case of extreme doxxing and harassment against a community manager for Bungie, Inc. ("Bungie"). Bungie employed the victim as a community manager for their video game, *Destiny 2*.¹⁰⁶ Community managers function "as an essential bridge between players and Bungie" and

100. Schubert, *supra* note 5, at 19.

101. *Id.*

102. *Id.*

103. 47 U.S.C. § 230(c)(1) (2018).

104. Schubert, *supra* note 5, at 19.

105. *Id.*

106. Default Judgment and Order at 3, *Bungie, Inc. v. Comer*, No. 22-2-10761-8 (Super. Ct. Wash. July 11, 2023).

promote the game in various ways.¹⁰⁷ The victim here, promoted the artwork of UhMaayze, a Black fan and creator of *Destiny 2* artwork.¹⁰⁸

The perpetrator of the doxxing and harassment, Comer, a disgruntled *Destiny 2* gamer, was “incensed” by the victim’s choice to highlight artwork by a person of color.¹⁰⁹ Comer proceeded to launch a harassment campaign on the victim and Bungie.¹¹⁰ Comer used the TextNow VoIP service to anonymously call the victim and the victim’s wife, leaving “hideous, bigoted,” and racist voicemails and sent the victim and his wife racist and threatening text messages.¹¹¹ Comer spent hours bombarding the victims with threatening and harassing phone calls and text messages.¹¹² Comer then escalated his harassment by threatening the victims by showing them “that he knew where they lived and could assault them there.”¹¹³ He placed an order for a pizza delivery that was to be cash on delivery and instructed the delivery driver to “knock at least five times” and to bang on the door insistently and loudly.¹¹⁴ After confirming the pizza was delivered via online tracking, Comer then texted the victim to “enjoy the pizza.”¹¹⁵ Bungie sent out executive protection after the pizza incident and notified police to safeguard the victims from Comer.¹¹⁶ In addition to the costs of executive protection, Bungie incurred costs during its attempt to ascertain Comer’s identity because it had to engage counsel in Canada, obtain a Canadian court order, retain additional legal counsel in West Virginia once they learned that was where Comer lived, and obtain a restraining order.¹¹⁷

In *Bungie, Inc. v. Comer*, Comer engaged in a pattern of online harassment that was likely to escalate from doxxing to contact through physical violence against the target.¹¹⁸ The harassment in this case could easily have culminated into tragedy via swatting or other real-world violence.¹¹⁹ The Washington court recognized the threat and danger posed by the conduct of doxxing by recognizing a new tort cause of action. The court stated “even if none of the above causes of action provided a basis for damage recovery where a malicious actor damages a company by intentionally targeting the company’s employees with harassment and threats, the court would exercise its authority to recognize a new common law tort that does.”¹²⁰ The court acknowledged that in many cases, individual employees would not have the resources available to uncover the anonymous harasser’s identity on their own and “[a]llowing employers to recover for protecting their employees

107. *Id.*

108. *Id.* at 3-4.

109. *Id.* at 4.

110. *Id.*

111. *Id.*

112. *Id.*

113. *Id.*

114. *Id.*

115. *Id.* at 5.

116. *Id.* at 6.

117. *Id.*

118. *Id.* at 5.

119. Tassi, *supra* note 6.

120. Default Judgment and Order at 11, *Bungie, Inc. v. Comer*, No. 22-2-10761-8 (Super. Ct. Wash. July 11, 2023).

from such harassment will give teeth to Washington's expressed public policy outlawing such harassment and encourage other employers to take similar steps when their employees are anonymously harassed online or over the phone."¹²¹

Washington's new tort differs from existing torts in combating doxxing and swatting because it gives employers a civil cause of action against malicious actors who harass and threaten their employees. The new tort allows companies to protect their employees from internet threats and harassment and help their employees uncover the people responsible for such threats. Washington's new tort allows companies to recover damages, including the investigative costs to uncover the perpetrator's identity and costs associated with providing security to its employees in the event of threats and harassment.¹²²

Other jurisdictions implementing their own new common law torts like Washington's would enable employers to assist their employees in identifying their harassers. Many victims lack the resources necessary to locate a perpetrator who has masked their identity. A tort giving a cause of action to employers for damage done to the company by targeting employees would allow companies with a large pool of resources to identify people responsible for their employees' doxxing and swatting.

2. *Oregon's Anti-Doxxing Statute*

In June 2021, Oregon enacted a new "anti-doxxing" statute to address the need for civil remedies for victims of this type of harassing conduct after "numerous concerning incidents where individuals have been doxed."¹²³ The statute is aimed at deterring and providing remedy for the improper disclosure of private information when there is intent to stalk or harass the victim. Oregon Revised Statute ("ORS") Section 30.835 provides:

A plaintiff has a cause of action for improper disclosure of private information if the plaintiff establishes by a preponderance of the evidence that: (a) The defendant, with the intent to stalk, harass or injure the plaintiff, knowingly caused personal information to be disclosed; (b) The defendant knew or reasonably should have known that the plaintiff did not consent to the disclosure; (c) The plaintiff is stalked, harassed or injured by the disclosure; and (d) A reasonable person would be stalked, harassed or injured by the disclosure.¹²⁴

ORS Section 30.835 defines personal information as: home addresses, email addresses, social security numbers, contact information of victim's employer, contact information of a family member of the victim, photographs of victim's children, and identification of the school that the doxxing victim's children attend.¹²⁵ Doxxing victims who prevail under a Section 30.835 claim can recover

121. *Id.* at 13.

122. *Id.*

123. *DeHart v. Tofte*, 533 P.3d 829, 834 (Or. Ct. App. 2023).

124. OR. REV. STAT. ANN. § 30.835(2)(a)-(d) (2021).

125. *Id.* § (1)(d)(A)-(E).

economic damages, noneconomic damages, punitive damages, injunctive relief, attorney fees, and any other appropriate equitable relief.¹²⁶

The statute differs from the common law tort of public disclosure of private facts in that the statute is tailored to doxxing or swatting victims. Section 30.835's personal information definition includes all the typical types of information found in a dox and language about intent to stalk, harass, or injure the plaintiff. The limitations of Oregon's anti-doxxing statute are that the remedy is limited to private individuals, not public officials, and the emotional distress from the harassment must be severe with the severity being analyzed on a basis of "duration and intensity."¹²⁷ Often, doxxing cases continue and escalate over a period of time, satisfying the duration aspect of the severity requirement of Section 30.835. Cases such as *Bungie, Inc. v. Comer* or the Obnoxious case previously discussed show-case the intensity aspect of the severity requirement of Section 30.835 because in those cases the doxxing was intense, threatening, and escalating towards physical attacks. In *Bungie*, the doxxing perpetrator consistently messaged and called them throughout the day, not just in a one-time incident; further, the perpetrator there had used the victim's address to intentionally harass, stalk, or injure the victims.¹²⁸ In Obnoxious's case, he committed dozens of doxxes on multiple female streamers, and had called in a swatting on many of them. His harassment of the victims lasted over a period of months, which, if under Oregon's jurisdiction, would satisfy the duration and intensity prongs of severity as required for the harassment under Section 30.835.¹²⁹

Oregon's anti-doxxing statute should be adopted in other jurisdictions as it can provide specific deterrence and remedy for doxxing harassment. Oregon State Senator James Manning stated the legislature's reasoning for enacting the anti-doxxing statute was because "[d]oxing is a tool used to hurt. House Bill 3047 will ensure those who choose to cause that hurt know they can be held accountable and will give tools to victims of this bullying tool to seek financial remedy."¹³⁰ Specific remedies aimed at doxxing and swatting are needed to enable victims of these kinds of harassment to be redressed for the significant injuries that can be caused. Causes of action tailored to doxxing and swatting can significantly assist in deterrence. Oregon's anti-doxxing statute does just that by explicitly addressing doxxing and giving victims of this conduct a civil cause of action.

3. Ontario's Internet Harassment Tort

In 2021, the Ontario Superior Court recognized a new tort of internet harassment in its decision in the case *Caplan v. Atas*.¹³¹ There, the new tort recognition

126. *Id.* § (3)(a)-(e).

127. *DeHart*, 533 P.3d at 886 (quoting *Checkley v. Boyd*, 14 P.3d 81, 94 (Or. Ct. App. 2000)).

128. Default Judgment and Order at 4, *Bungie, Inc. v. Comer*, No. 22-2-10761-8 (Super. Ct. Wash. July 11, 2023).

129. Fagone, *supra* note 19; see also § 30.835.

130. *Oregon Lawmakers Send 'Anti-Doxing' Legislation to Governor's Desk*, KTVZ NEWS (June 7, 2021, 2:03 PM), <https://ktvz.com/news/oregon-northwest/2021/06/07/oregon-lawmakers-send-an-anti-doxing-legislation-to-governors-desk/>.

131. Warwick & Cameron, *supra* note 6.

arose out of the defendant's "'extraordinary' campaigns of cyber-stalking, harassment, and defamation."¹³² The extreme internet harassment in this case continued over two decades and consisted of the harasser making malicious falsehoods by posting anonymously on social media platforms.¹³³ The Ontario court concluded none of their current torts sufficiently addressed the conduct at bar. They acknowledged current torts provided some remedy to victims but were not completely "sufficient to end the conduct or control the behaviour."¹³⁴

Ontario's tort of internet harassment adopts a three-part test to establish a claim: (1) the defendant maliciously or recklessly engages in communications conduct so outrageous in character, duration, and extreme in degree, so as to go beyond all possible bounds of decency and tolerance; (2) the defendant intends to cause fear, anxiety, emotional upset or to impugn the dignity of the plaintiff; and (3) the plaintiff suffers such harm.¹³⁵ The court further provided that this new tort is not for "conduct intended to annoy" but is to be reserved for "only the most 'serious and persistent of harassing conduct.'"¹³⁶ The Ontario court granted the plaintiffs in the *Caplan* case a "permanent injunction preventing the defendant... from posting about the plaintiffs, their families, and their business associates on the internet... [and] vested title in the existing posts in the plaintiffs, so they could take the necessary steps to have the content removed from the internet."¹³⁷

The novel internet harassment tort recognized in Ontario is very similar to IIED. To have a claim for IIED, the elements are: "(1) extreme and outrageous conduct; (2) intent or recklessness; (3) causation; and (4) severe emotional distress."¹³⁸ To have a claim under Ontario's internet harassment tort, one must show:

1. The defendant maliciously or recklessly engaged in communications so outrageous in character, duration and extreme in degree, so as to go beyond all possible bounds of decency and tolerance;
2. The defendant acted with the intent to cause fear, anxiety, emotional upset or to impugn the dignity of the plaintiff; and
3. The plaintiff suffered such harm.¹³⁹

IIED and Ontario's internet harassment tort have similar elements required to have a claim under the tort because they both require (1) extreme and outrageous conduct, (2) intent or recklessness, and (3) that the plaintiff suffered the required harm. Ontario's internet harassment tort differs from a traditional IIED claim in that it merely requires the plaintiff suffer fear, anxiety, emotional upset, or

132. *Id.*

133. *Id.*

134. *Id.*

135. *Id.*

136. *Id.*

137. *Id.*

138. *Duran v. Detroit News*, 504 N.W.2d 715, 720 (Mich. Ct. App. 1993).

139. Gillian P. Kerr & William Main, *The Tort of Internet Harassment: A New Tort with an Extraordinary Remedy*, MCCARTHY TETRAULT (Feb. 8, 2021), <https://www.mccarthy.ca/en/insights/blogs/techlex/tort-internet-harassment-new-tort-extraordinary-remedy#>.

impugned dignity to have an actionable claim, as opposed to IIED requiring the high bar of extreme emotional distress suffered by the plaintiff. Ontario's internet harassment tort lessens the harm requirement in a way that helps victims of doxxing and swatting. IIED claims can be difficult to establish because requiring proof of severe emotional distress sets a high bar for these claims.¹⁴⁰ The Ontario tort alleviates this difficulty for victims of doxxing, swatting, and other types of harassment by allowing them to establish their claim with only proof of fear, anxiety, and emotional upset or impugned dignity.¹⁴¹ This new tort, if recognized widely, would provide victims of these forms of harassment with a civil cause of action that is easier to establish and would give victims an opportunity to receive remedy for their injuries without having to establish the high bar of severe emotional distress set by IIED.

In addition to the Ontario tort making it easier to establish claims, the tort also enables victims to receive the remedy of having title of the offending postings or accounts transferred from the offender to them.¹⁴² This remedy allows victims to have the harassing content removed from websites. In a doxxing situation, this tort remedy would allow the victim to have their personal information removed from malicious forums and could prevent their information from being used for swatting or other real-world harms in the future.

The above discussed new developments in the law should be considered by other jurisdictions. States should recognize a tort cause of action that specifically targets internet harms. Victims of doxxing and swatting can suffer significant injury that could be completely remedied by adoption of some variation of the above internet harassment laws. New internet harassment torts will not only serve to redress the injuries of victims of doxxing or swatting, but also could be used to deter and remedy victims of other kinds of cyberbullying and harassment. People are increasingly online in today's world, which coincides with the increase in online harm committed. These increases call for laws that specifically address harm committed in the cyber world. Doxxing and swatting may be within the compass of current tort causes of action, but there is no widely recognized tort that specifically addresses this kind of behavior.

CONCLUSION

Doxxing and swatting are a significant issue in today's increasingly online world. These forms of online harassment are popular tools for cyber abusers in the world of gaming and video game streaming; however, anyone can find themselves as a victim of doxxing and swatting for a multitude of banal reasons. Current tort law frameworks, such as intentional infliction of emotional distress, and invasion of privacy torts, such as intrusion upon seclusion and public disclosure of private facts, may provide victims with some remedy, but the significant increase in these malicious behaviors suggests more civil remedies are needed. Doxxing

140. *Brown v. Bank*, 2022 WL 657564, at *16 (D. Md. 2022) (citing *Bagwell v. Peninsula Reg'l Med. Ctr.*, 665 A.2d 297, 319 (Md. Ct. Spec. App. 1995)).

141. *Kerr & Main*, *supra* note 139.

142. *Id.*

and swatting can cause serious tortious harm to victims, and while these types of harassment fall into the scope of currently recognized torts, a tort cause of action specifically designed to target online harassment is necessary to provide victims with complete remedy and to further deter these behaviors.

To combat the harms of malicious online harassment in the form of doxxing and swatting, jurisdictions such as Oregon, Washington State, and Ontario, Canada have recognized new civil causes of action specifically aimed at deterring online or internet harassment. Other jurisdictions nationwide should recognize online harassment torts modeled after those discussed above to provide victims of doxxing and swatting with an adequate remedy for their damages and to address and deter modern harms. Swatting and doxxing is a significantly growing form of harassment and can cause serious harm to victims and, as such, requires specifically tailored tort causes of action to address that serious harm.

Therefore, state legislators should seek to create new modern torts that are distinctly aimed at targeting online tortious harassment to provide a more complete remedy to victims of doxxing and swatting. The above evolutions in the law surrounding tortious online harassment in the form of doxxing and swatting are a great step forward towards reducing these forms of harm and redressing the injury to victims of such harm.