Brooklyn Journal of International Law

Volume 42 | Issue 1 Article 8

2016

Making the Time Fit the Crime: Clearly Defining Online Harassment Crimes and Providing Incentives for Investigating Online Threats in the Digital Age

A. Meena Seralathan

MAKING THE TIME FIT THE CRIME: CLEARLY DEFINING ONLINE HARASSMENT CRIMES AND PROVIDING INCENTIVES FOR INVESTIGATING ONLINE THREATS IN THE DIGITAL AGE

INTRODUCTION

On August 16, 2014, Zoe Quinn was drawn into one of the most extensive incidents of cyberharassment in the United States when her ex-boyfriend, Eron Gjoni, posted a series of blog posts depicting, in meticulous detail, a story of how Quinn previously cheated on him.[1] The blog posts included intimate information that Quinn sent Gjoni in confidence, private Facebook correspondence between the two over the span of their relationship, and subjective commentary on the relationship by Gjoni. In his commentary, Gjoni included accusations that Quinn received acclaim for her self-published video game, *Depression Quest*, as a result of her affairs.[2] The accusations that Quinn received positive reviews for her video game as a result of her relationship with a video game journalist were soon proven false, as the man with whom she had an affair did not actually review her video game.[3] This, however, did not stop numerous Internet users from responding angrily to the blog posts.[4] In retaliation

---

1. Eron Gjoni, *TheZoePost*, WORDPRESS (Aug. 6, 2014), https://thezoepost.wordpress.com.

2. *Id.*; Caitlin Dewey, *The Only Guide to Gamergate You Will Ever Need to Read*, WASH. POST (Oct. 14, 2014), https://www.washingtonpost.com/news/the-intersect/wp/2014/10/14/the-only-guide-to-gamergate-you-will-ever-need-to-read. Gjoni's publishing of private information could constitute cyberharassment, depending on the jurisdiction one examines. *See infra* Parts I, II.

3. *See* Abigail Elise, *What is the GamerGate Scandal? Female Game Developer Flees Home Amid Online Threats*, INT'L BUS. TIMES (Oct. 13, 2014, 3:27 PM), http://www.ibtimes.com/what-gamergate-scandal-female-game-developer-flees-home-amid-online-threats-1704046.

4. Numerous Internet users banded together in a movement called #Gamergate. *See id.* Allegedly formed to address ethics in journalism as a result of Quinn's affair, #Gamergate became associated with repeated attacks against Quinn and other female game developers or journalists who publically supported Quinn. *See id.*; *see also* Dewey, *supra* note 2.

to her alleged behavior and favored treatment, anonymous hackers[5] released Quinn's personal information (including her home address, her phone number, and private nude photographs) to the public.[6] Quinn also received numerous rape threats and threats of violence, and Quinn's website faced multiple hacking attempts.[7] Ultimately, Quinn fled her home and sought a restraining order against Gjoni, which was quickly challenged in court.[8]

Cybercrimes that involve online harassment, such as cyberharassment and cyberstalking, are becoming ever more prevalent as people become more and more active on the Internet.[9] In particular, in 2012 alone, at least nine million women reported

5. While not a focus of this Note, Internet mobs (e.g., groups of people online who commit harassment or stalking campaigns online) are also becoming increasingly important to address, in and of themselves, through additional legislation, due to the proliferation of Internet usage across the globe. For further information about Internet mobs, see Michael Barrett Zimmerman, *One-Off & Off-Hand: Developing an Appropriate Course of Liability in Threatening Online Mass Communication Events*, 32 CARDOZO ARTS & ENT. L.J. 1027, 1036–42 (2014).

6. Elise, *supra* note 3; Dewey, *supra* note 2; Sarah Kaplan, *With #GamerGate, the Video-Game Industry's Growing Pains Go Viral*, WASH. POST (Sept. 12, 2014), http://www.washingtonpost.com/news/morning-mix/wp/2014/09/12/with-gamergate-the-video-game-industrys-growing-pains-go-viral.

7. *See* Kaplan, *supra* note 6.

8. *See* Dewey, *supra* note 2; Eugene Volokh, *'You Are Also Ordered Not to Post Any Further Information About the [Plaintiff],'* WASH. POST (Aug. 24, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/08/24/you-are-also-ordered-not-to-post-any-further-information-about-the-plaintiff.

9. In many countries, including but not limited to the United States, the United Kingdom, and India, instances of cyberharassment and cyberstalking are on the rise. *See* CARSTEN MAPLE, EMMA SHORT, & ANTONY BROWN, CYBERSTALKING IN THE UNITED KINGDOM 15 (2011), http://www.beds.ac.uk/__data/assets/pdf_file/0003/83109/ECHO_Pilot_Final.pdf; Karen McVeigh, *Cyberstalking 'Now More Common' Than Face-to-Face Stalking*, GUARDIAN (Apr. 8, 2011, 1:31 PM), http://www.theguardian.com/uk/2011/apr/08/cyberstalking-study-victims-men; Amrita Madhukalya, *Online Harassment of Women is on the Rise*, DNA (July 29, 2014, 6:20 AM), http://www.dnaindia.com/india/report-online-harassment-of-women-is-on-the-rise-2006090; Stefan Hankin, *The Rise of Online Harassment*, POLITICUS (June 27, 2014), http://thepoliticus.com/content/rise-online-harassment.

being a victim of cyberstalking in the European Union,[10] and at least 1.5 million U.S. citizens reported being victims of cyberharassment in 2010.[11] Both average citizens and celebrities alike have become targets of online attacks.[12]

Legal remedies for victims of cyberharassment and cyberstalking, however, can be limited.[13] For example, in Massachusetts (Quinn's state of residence), prosecutors would be unable to win a cyberharassment case against Gjoni because of the narrow statutory definition of harassment.[14] Additionally, while Quinn

---

10. Katherine Quarmby, *How the Law is Standing Up to Cyberstalking*, NEWSWEEK (Aug. 13, 2014, 6:08 AM), http://www.newsweek.com/2014/08/22/how-law-standing-cyberstalking-264251.html.

11. Bennet Kelley, *The Unbearable Unawareness of Cyber-Harassment*, HUFFINGTON POST (Mar. 27, 2010, 5:12 AM), http://www.huffingtonpost.com/bennet-kelley/the-unbearable-unawarenes_b_434484.html.

12. *See* Dewey, *supra* note 2; Caitlin Dewey, *A Vengeful Internet Trashed the Yelp Page of the Minnesota Dentist Who Shot Cecil the Lion*, WASH. POST (July 28, 2015), https://www.washingtonpost.com/news/the-intersect/wp/2015/07/28/a-vengeful-internet-trashed-the-yelp-page-of-the-minnesota-dentist-who-shot-cecil-the-lion/; Nick Watt, *Celebrities and Cyberstalkers: The Dark Side of Fame in the Internet Age*, ABC NEWS (July 9, 2012), http://abcnews.go.com/Technology/celebrities-cyberstalkers-dark-side-fame-internet-age/story?id=16741230; Hayley Tsukayama, *Twitter Vows to "Improve Our Policies" After Robin Williams' Daughter is Bullied Off the Network*, WASH. POST (Aug. 13, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/08/13/twitter-vows-to-improve-our-policies-after-robin-williams-daughter-is-bullied-off-the-network/.

13. Volokh, *supra* note 8.

14. Massachusetts law requires "willfully and maliciously engaging in a knowing *pattern* of conduct or series of acts over a period of time." MASS. ANN. LAWS ch. 265, § 43A(a) (LexisNexis 2016) (emphasis added). Massachusetts courts have ruled that at least three acts committed on different days can constitute a series of acts over a period of time (*see, e.g.*, Commonwealth v. Welch, 444 Mass. 80, 89 (2005); Commonwealth v. Robinson, 444 Mass. 102, 109 (2005)) but have not, so far, indicated whether multiple blog posts published in succession on the same day (e.g., as Gjoni's original posts were published) would qualify as "a knowing pattern . . . or series of acts." ch. 265, § 43A(a). In fact, in *Robinson*, the court described the defendant's act of stopping his car near the victim twice in the same day to glare "menacingly" at her as being part of one "incident." *Robinson*, 444 Mass. at 109. This would suggest that repetition of the same form of harassment, in the same day, may not fall under the state's definition of a pattern or series of acts over a period of time. Even if the actions had occurred on different days, however, it would still be difficult to prove malicious or similar intent in cases involving online harassment. *See infra* Part III.

did attempt to obtain a restraining order against Gjoni in Massachusetts state court[15] to prevent him from speaking further about Quinn's personal life or any other details that would further fuel online harassment against her, this restraining order is currently being challenged on First Amendment grounds.[16] Legal scholars have argued, for example, that Gjoni has a First Amendment right to talk about his relationship with Quinn and to talk about Quinn herself, and that his right to do so should not be stifled by what other malicious actors do with that information.[17] If the unconstitutionality argument proves to be persuasive to the court, Quinn would also be unable to maintain a restraining order against Gjoni to prevent him from disclosing additional private conversations between himself and Quinn.[18] If Quinn cannot maintain such a restraining order, other victims may not be able to use restraining orders to prevent people from disseminating personal information about them online.

---

15. Volokh, *supra* note 8 ("[A] Massachusetts trial court issued an order providing that Gjoni is 'Ordered not to post any further information about the [plaintiff] or her personal life on line or to encourage 'hate mobs.'").

16. Eugene Volokh and Aaron Caplan helped file a "friend-of-the-court brief" in the case (now at the appellate level). *See id.* Volokh argued against a restraining order Quinn filed against Gjoni, arguing that preventing Gjoni from posting anything about Quinn, her personal life, or anything that would encourage further hate mobs would constitute "unconstitutional prior restraint." *See id.* Prior restraint generally refers to a judicial prohibition or restriction on particular expression, such as an injunction on speaking on a particular matter. *See generally* Chicago Council of Lawyers v. Bauer, 522 F.2d 242, 248 (7th Cir. 1975). Thus, Volokh's argument, therefore, was that preventing Gjoni from talking about Quinn would be an unconstitutional judicial exercise in restricting Gjoni's speech, and therefore that a restraining order preventing Gjoni from speaking about Quinn would be unconstitutional.

17. *See* Volokh, *supra* note 8.

18. Volokh argues that there are "many possible legal actions that might be contemplated here." *Id.* Many of these options fall outside the focus of this Note. It should be noted, however, that Volokh acknowledges that many of the suggestions he provides are also unrealistic for someone in Quinn's position. For example, Volokh concedes that, though Quinn could sue for disclosure of her personal information, "the 'disclosure of private facts' tort . . . is quite narrow and complex." *Id.* Further, "it's often hard to track . . . down [people who send death threats]," and though in theory one can already be convicted of a crime to incite others to perform criminal conduct against another, "that's an extremely narrow First Amendment exception." *Id.* Volokh's concession that his alternative options depend on relying on difficult and narrow rules and exceptions punctuate why existing law is ill-equipped to help victims like Quinn.

Pursuing legal remedies against anonymous hackers who release personal information or send death threats can be hampered by law enforcement's lack of motivation to use limited resources to identify anonymous actors.[19] A former Federal Bureau of Investigations (FBI) supervisory special agent previously involved with cybercrimes investigations suggested that the unique difficulties of tracking anonymous perpetrators of cyberharassment, coupled with minor punishments for such crimes, discourage officials from taking certain steps to fully investigate cyberharassment cases.[20] Identifying perpetrators requires the use of computer forensics specialists to trace a user's online account to their actual identity (e.g., through their Internet Protocol (IP) address or through more complicated means when an IP address is not enough to definitively identify the user).[21] This identification process can be time-intensive and requires training or contracts with outside investigative agencies, which can result in significant cost to law enforcement agencies.[22] Because punishments for cyberharassment often do not justify the time and resources required to identify a potential harasser, local police and FBI agents are less likely to prioritize state or federal cases (respectfully) against people who anonymously commit online crimes.[23] Investigations, however, can be essential for establishing the basic elements of laws that criminalize online harassment and stalking and for ultimately bringing successful cases against perpetrators of online harassment and stalking. For example, when threats are anonymous, it can be difficult to determine whether the threats are the result of a single person issuing multiple threats or whether each threat is a singular instance of different users lashing out at a victim. This distinction

---

19. Amanda Hess, *A Former FBI Agent on Why It's So Hard to Prosecute Gamergate Trolls*, SLATE (Oct. 17, 2014, 4:23 PM), http://www.slate.com/blogs/xx_factor/2014/10/17/gamergate_threats_why_it_s_so_hard_to_prosecute_the_people_targeting_zoe.html.

20. *Id.*

21. Caitlin Dewey, *Why is it Taking so Long to Identify the Anonymous Gamergate Trolls?*, WASH. POST (Oct. 17, 2014), https://www.washingtonpost.com/news/the-intersect/wp/2014/10/17/why-is-it-taking-so-long-to-identify-the-anonymous-gamergate-trolls.

22. Hess, *supra* note 19.

23. According to former FBI agent Tim Ryan, "[s]pending a month getting subpoenas and doing wiretaps for a case where the sentence is six months of probation just doesn't make sense." Hess, *supra* note 19.

can be a crucial element to prove in a criminal case, as many states require the threats to be of a specific nature (i.e., to involve multiple threats, to involve one perpetrator, or to involve multiple perpetrators) before a crime has been committed.[24] It therefore becomes that much harder to prove a cyberharassment or cyberstalking case when law enforcement is uninterested in spending large amounts of time or resources to investigate a potential crime that carries a low-level sentence.

Even if a victim's local law enforcement is willing to use their resources to identify cyberharassers and cyberstalkers, trying to understand one's legal recourse can be daunting for persons handling such cases.[25] Specifically, a complete lack of a unified standard for cyberharassment and cyberstalking crimes across various jurisdictions in the United States and across the globe (particularly when cyberharassers and cyberstalkers can exist in any jurisdiction in the world) can lead to some ambiguity and inconsistency as to how various courts may treat a given cyberharassment or cyberstalking case.[26] State and federal jurisdictions of the United States have widely varying definitions of cyberharassment and cyberstalking as well as different standards for determining the intent of the accused.[27] In the United States, while there are some statutes that cover certain forms of cyberharassment and cyberstalking, existing state statutes can vary widely from state to state (causing inconsistencies in how victims, cyberharassers, and cyberstalkers are treated under the law). Further, the few federal statutes available to address cyberharassment and cyberstalking are either inadequate for addressing what Quinn and many other victims have faced, or have been made even more difficult to prove or interpret by recent court decisions.[28] In countries such as Canada, there is a

---

24. Massachusetts law, as noted above, requires some "knowing *pattern* of conduct or *series of acts* over a period of time." MASS. ANN. LAWS ch. 265, § 43A(a) (LexisNexis 2016) (emphasis added). If Quinn cannot prove that different instances of harassment came from the same person, then she cannot prove that any of the anonymous users conducted a pattern of harassment or committed several acts of harassment.

25. *See* Aimee Fukuchi, *A Balance of Convenience: The Use of Burden-Shifting Devices in Criminal Cyberharassment Law*, 52 B.C. L. REV. 289 (2011).

26. *See id.*

27. *State Legislation*, KIDSBESAFEONLINE (2009), http://www.kidsbesafeonline.com/state-legislation.html.

28. *See infra* Part II.A; *see also* Elonis v. United States, 135 S. Ct. 2001 (2015).

similar range of variance between federal and provincial laws.[29] Internationally, there is no treaty that would allow a victim such as Quinn to seek remedies from any international cyberharassers or cyberstalkers who attacked her.[30] The Council of Europe's Convention on Cybercrime is the leading cybercrime treaty, but handles a very narrow subset of cybercrimes that do not fully include different forms of online harassment.[31]

Thus, an analysis of numerous examples of cyberharassment and cyberstalking laws in the world can provide a guide for reforming U.S. laws specifically, and cyberharassment and cyberstalking laws generally. For example, examining the numerous laws in the United States, including various state laws and federal laws, such as the Interstate Communications Act (ICA), the Communications Act ("CA"), and the Interstate Stalking Punishment and Prevention Act (ISPPA) can offer strategies for amending existing laws to ensure U.S. citizens, like Zoe Quinn, have legal recourse for online attacks.[32] Examining Canada's recent battles with online harassment with respect to its federal Criminal Code, Nova Scotia's Cyber-Safety Act (CSA), and Ontario's civil tort law have demonstrated the extent to which concerns relating to First Amendment rights interact with the goals of protecting victims from online harms, thus offering glimpses into potential pitfalls of passing similar statutes in the United States.[33] Finally, examining Australia's federal cyberharassment law (in particular, its sentencing structure, its intent standards, and its overall definition of cyberharassment and cyberstalking crimes) can provide insight into an alternative legal framework that offers potential solutions to a number of the issues faced by other jurisdictions struggling to address cyberharassment and cyberstalking.[34] Existing laws demonstrate both the extent to which individual nations, and the world at large, have to go in terms of enacting helpful cyberharassment and cyberstalking legislation and potential avenues for better addressing such crimes.

---

29. *See infra* Part III.B.1.

30. *See infra* Part II.B.1.

31. *Details of Treaty No.185,* COUNCIL EUR., http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (last visited Jan. 17, 2017).

32. *See infra* Part III.A.

33. *See infra* Part III.B.1.

34. *See infra* Part III.B.2.

In trying to address the widely different and sometimes problematic definitions of cyberharassment and cyberstalking, and in trying to motivate law enforcement to investigate cyberharassment and cyberstalking crimes, this Note proposes a U.S. Federal Model Statute ("Model Statute") that uses elements of laws enacted throughout the United States and in other Western countries, such as Canada and Australia, to consolidate definitions of cyberharassment and cyberstalking into one federal law and to amend sentencing structures for existing law to motivate law enforcement to investigate such crimes. Specifically, the proposed Model Statute is designed to move the United States toward an objective standard for these cybercrimes (i.e., a standard that relies on what a reasonable person would believe or perceive, rather than what the persons in the alleged incident subjectively believed or perceived), making it easier to prosecute anonymous persons for whom intent may be difficult to prove. Additionally, the proposed Model Statute is designed to make investigations of these cybercrimes more palpable for U.S. law enforcement by conforming and raising statutory punishments for cyberharassment and cyberstalking to be consistent with those enacted by other Western countries (such as Australia[35] and Canada[36]).

Part I of this Note will examine the current state of cyberharassment and cyberstalking legislation in the United States and abroad, including ways in which cyberharassment and cyberstalking are defined and examples of how such cybercrimes can affect victims in ways that traditional crimes may not. Part II of this Note will look at existing laws in the United States and abroad—such as state and provincial laws within the United States and Canada, respectively, federal laws within the United

35. The Australian legal system provides an interesting glimpse into how to address attacks across state lines (or potentially even attacks across national lines) and sentencing schemes that may help law enforcement justify prioritization of cybercrimes. For example, Australian federal cybercrime laws include provisions for prosecuting crimes involving out-of-state parties and a tiered-sentencing system. *See generally infra* Part II.B.2.

36. Canada serves as a useful case study on potential First Amendment challenges to cyberharassment statutes that criminalize extremely broad categories of online harassment, which has the effect of limiting speech. *See generally Halifax Lawyer to Launch Charter Case Challenge of Cyber-Safety Act*, CBC NEWS (Aug. 15, 2015, 4:08 PM), http://www.cbc.ca/news/canada/nova-scotia/halifax-lawyer-to-launch-charter-case-challenge-of-cyber-safety-act-1.3192440.

States, Canada, and Australia, and an international treaty—that attempt to address cyberharassment and cyberstalking. Specifically, Part II will assess the wide variety of definitions of cyberharassment and cyberstalking that exist both within nations and between nations as well as the different ways in which jurisdictions punish cyberharassers and cyberstalkers. Part III of this Note will discuss how the laws in the United States and Canada fail to adequately address issues arising from the prevalence of cyberharassment and cyberstalking (e.g., by failing to cover certain forms of cyberharassment and cyberstalking or by including provisions that impact the enforceability of the applicable laws). Part IV of this Note will propose a Model Statute to provide uniformity in applying cyberharassment and cyberstalking laws to U.S. citizens and to address the ambivalence by law enforcement to investigate instances of cyberharassment and cyberstalking.

I. BACKGROUND OF CYBERHARASSMENT AND CYBERSTALKING

Innovations of Internet technology have created new tactics and forms of harassment that were not feasible, or even possible, in instances of offline harassment. Understanding the ways in which the Internet can fundamentally change the nature of harassment (including how it is conducted, its prevalence, and its effects on its victims) is crucial to understanding how to prevent instances of future cyberharassment and cyberstalking.

A. Definitions of Cyberharassment and Cyberstalking

Cyberharassment has been defined in various ways by different scholars,[37] but is generally defined as "the use of email, instant messaging, and derogatory websites to bully or otherwise harass an individual or group through personal attacks."[38] The term "cyberharassment" can be considered synonymous with "cyberstalking,"[39] where cyberstalking generally refers to

37. *See Defining a Cyberbully: Social Scientists Struggle to Characterize New Form of Harassment*, NAT'L SCI. FOUND. (Nov. 8, 2011), http://nsf.gov/discoveries/disc_summ.jsp?cntn_id=121847&org=NSF.

38. *Cyber Harassment Law and Legal Definition*, USLEGAL, http://definitions.uslegal.com/c/cyber-harassment/ (last visited Feb. 12, 2017).

39. *See Cyberbullying/Stalking & Harassment*, WIREDSAFETY (2012), https://www.wiredsafety.org/subjects/cyberbullying.php.

"threatening, harassing, or annoying someone" in repeated encounters.[40] In other words, cyberharassment may include a one-time incident of name-calling, threatening a victim, or releasing private information, whereas cyberstalking includes multiple instances of tracking a person online or committing multiple acts of cyberharassment against a particular person.[41]

Cyberharassment and cyberstalking can also materialize in different ways. Hacking attempts, publication of personal information on the Internet, name-calling, rape threats, or other threats of violence all constitute forms of cyberharassment.[42] In instances of cyberharassment or cyberstalking, a victim's private social media and text messages, real name, email address, phone number, residential address, nude photographs, and other such information may be posted online to encourage dissemination of the victim's personal information.[43] Cyberharassment can be perpetrated by a single person[44] or by a number of persons acting against one or more victims.[45] The accused can be known to the victim or can be an anonymous entity that the victim cannot identify.[46]

Harassment and stalking in and of themselves are not new crimes in U.S. discourse; their cyber counterparts, however, can involve unique complications.[47] While information can spread without the use of technology, social media and other forms of online communication allow information to be shared with a

---

40. *Cyberstalking Law and Legal Definition*, USLEGAL, http://definitions.uslegal.com/c/cyberstalking/ (last visited Feb. 12, 2017).

41. *See Cyberbullying/Stalking & Harassment*, *supra* note 39. Cyberharassment is not considered the same as "cyberbullying," a term generally used in the United States to describe conduct between minors. *See id.*

42. *See* Kaplan, *supra* note 6.

43. *See* Elise, *supra* note 3; Dewey, *supra* note 2; Kaplan, *supra* note 6.

44. In Zoe Quinn's case, Gjoni arguably committed cyberharassment because he personally released several pages of private correspondence and other information about Quinn's private life. *See* Gjoni, *supra* note 1.

45. *See* Dewey, *supra* note 2.

46. *See generally* Quarmby, *supra* note 10. An anonymous perpetrator can be more difficult to identify than a known perpetrator, causing additional costs or training needs on the part of law enforcement or the victim to identify persons so that legal remedies can be pursued. As noted above, if law enforcement lacks the resources to investigate a cyberharassment case, they are unlikely to prioritize it over other types of cases. *See* Hess, *supra* note 19.

47. *See* JAMES GRIMMELMANN, INTERNET LAW: CASES AND PROBLEMS 159 (5th ed. 2015).

simple click of a button.[48] Thus, because distribution of content on the Internet is easier and faster than its nondigital equivalents, threats and personal information shared without permission can persist online longer, can be shared faster, can be viewed by more people in a shorter span of time, and can be searchable by using search engines or other means.[49] Furthermore, cybercrimes are not constrained by geography; perpetrators can harass or stalk online victims across state or even national lines.[50]

Additionally, the Internet can cause new complications in terms of identifying perpetrators. Online profiles are typically anonymous, as people often use online pseudonyms instead of their real identities.[51] In the context of cyberharassment, a 2014 study by Pew Research Center indicated that at least 26 percent of respondents did not know the real identity of their harasser at all, and 38 percent of respondents indicated that their harasser had been a stranger to them.[52] Normally, law enforcement attempts to counteract this by determining the IP address of anonymous users.[53] When the user's device is connected to the Internet, an IP address serves as a unique identifier linked to a

---

48. *See id.* at 159–60.

49. *See id.*

50. *See* Quarmby, *supra* note 10.

51. Martin Clear, *Why Should I Reveal My 'Real Identity' Online? Anonymity Isn't So Terrible*, GUARDIAN (Jan. 15, 2014, 7:21 AM), http://www.theguardian.com/commentisfree/2014/jan/15/reveal-real-identity-online-anonymity.

52. *See* Maeve Duggan, *Online Harassment*, PEW RES. CENT. (Oct. 22, 2014), http://www.pewinternet.org/files/2014/10/PI_OnlineHarassment_72815.pdf. Perhaps surprisingly, only 10% of respondents indicated that the harasser was a previous romantic partner. *Id.* at 26. In a different 2013 study, 51% of victims of cyberstalking were single, and 60% of victims of cyberstalking were women. *See 2013 Cyberstalking Statistics*, WORKING TO HALT ONLINE ABUSE, http://www.haltabuse.org/resources/stats/2013Statistics.pdf (last visited Feb. 12, 2017); McVeigh, *supra* note 9. Though only 10% of respondents indicated that an ex-partner was their harasser, the study indicated that 47% of cyberstalkers in particular were ex-partners. *See 2013 Cyberstalking Statistics*, *supra* note 52. This meant, however, that 30% of respondents in the study were harassed or stalked online by an anonymous cyberharasser or cyberstalker. *See 2013 Cyberstalking Statistics*, *supra* note 52; McVeigh, *supra* note 9.

53. *See* GRIMMELMANN, *supra* note 47, at 292. For more information on IP addresses, see Rus Shuler, *How Does the Internet Work?*, SHULERS (2005), http://www.theshulers.com/whitepapers/internet_whitepaper/index.html; *IP Address*, TECH TERMS http://techterms.com/definition/ipaddress (last updated Sept. 21, 2016); J. Touch, *Updated Specification of the IPv4 ID Field*, TOOLS.IETF.ORG (Feb. 2013), https://tools.ietf.org/html/rfc6864.

user's device, allowing law enforcement to identify a user (through the device) even if one is utilizing an online pseudonym.[54] It is possible, however, for users to forge their IP address; the IP address, therefore, may not always be a reliable means to identify a particular user.[55] Additionally, there are various technologies that can be used to mask one's IP address.[56] For example, an Internet user can send messages through a "proxy," such that the message appears to come from an alternate, proxy device instead of from the user's device.[57] A user can use multiple proxies to further obfuscate her IP address.[58] As a result of these unique and complex ways to circumvent identification technology, law enforcement must typically hire employees with expertise in Internet technology and investigations of online criminal activity to identify perpetrators of cyberharassment and cyberstalking.[59] The prevalence of anonymous users abusing their victims thus demonstrates why it is crucial to implement measures that encourage law enforcement to investigate these crimes, even when additional resources, such as employees or training, will be necessary to investigate the crimes.

B. Effects of Cyberharassment and Cyberstalking

Cyberharassment can affect people of all genders, ages, and races, though some forms of cyberharassment can affect certain demographics more than others.[60] In a 2014 Pew Research Center survey,[61] 44 percent of men and 37 percent of women indicated that they had experienced some form of online harassment

54. *See* GRIMMELMANN, *supra* note 47, at 292; *see also* Shuler, *supra* note 53; *IP Address*, *supra* note 53; Touch, *supra* note 53.

55. *See* GRIMMELMANN, *supra* note 47, at 292.

56. *See* Stefan Larsson et al., *Law, Norms, Piracy and Online Anonymity: Practices of De-identification in the Global File Sharing Community*, 6 J. RES. INTERACTIVE MARKETING 260, 263 (2012).

57. *Id.*; *see also* Chris Hoffman, *How to Browse Anonymously with Tor*, HOW-TO-GEEK (May 15, 2012), http://www.howtogeek.com/114004/how-to-browse-anonymously-with-tor/.

58. *See* Larsson et al., *supra* note 56; Hoffman, *supra* note 57. It should be noted that such services, known as Tor services, frequently do serve purposes other than shielding Internet users from criminal liability. For more information on Tor services specifically, see *Tor: Overview*, TORPROJECT, https://www.torproject.org/about/overview.html.en (last visited Jan. 17, 2016).

59. *See* Hess, *supra* note 19.

60. *See* Duggan, *supra* note 52; *2013 Cyberstalking Statistics*, *supra* note 52.

61. The Pew Research Center is a U.S. nonpartisan organization that conducts "public opinion polling, demographic research, media content analysis

in their lifetime.[62] Men were more likely to experience less severe forms of harassment,[63] such as name-calling and embarrassment, while women were more likely to experience extreme forms of online harassment, such as stalking or sexual harassment.[64] Different genders may also often experience different fears associated with cyberharassment and cyberstalking.[65] For example, women are more likely to fear physical violence to themselves or to their loved ones.[66] On the other hand, men are more likely to fear damage to their reputation.[67]

The effects of cyberstalking can also be as varied as they can be severe. Victims can experience anxiety, a loss of personal safety, defamation of their character, damage to their professional reputation, alienation from their community, difficulties in child custody and other legal proceedings, depression, panic

---

and other empirical social science research." Duggan, *supra* note 52, at 1. The Pew Research Center establishes nationally representative panels of randomly selected U.S. adults to solicit survey participants. *See id.* at 62. The Online Harassment survey referenced herein, in particular, was self-administered via the internet by 2,849 Internet users included in such a panel between May 30 and June 30, 2014. *See id.* at 9. This number equated to approximately 60 percent of online panel participants. *Id.* at 63. The Pew Research Center calculated a margin of error of ±2.4. *Id.* at 9.

62. *Id.* at 13. The six forms of online harassment tracked in the survey include: "[n]ame-calling and embarrassment . . . sexual harassment, physical threats, sustained harassment, and stalking." *Id.* at 12.

63. While, in comparison, men do not face more severe forms of harassment as often as women, men unmistakably can also face vicious forms of harassment. In 2015, after becoming notorious for luring and killing a protected lion from a sanctuary, anonymous Internet users relentlessly harassed Walter Palmer in retaliation for his actions. *See* Lisa Green, *Walter Palmer, Cecil the Lion, and the Legality of Cyber-Bullying*, MSNBC (Aug. 10, 2015, 8:14 AM), http://www.msnbc.com/msnbc/walter-palmer-cecil-the-lion-and-the-legality-cyber-bullying; Dewey, *supra* note 12. The anonymous users littered his dental practice's Yelp page with death threats and other negative reviews, hacked his practice's dental website so that it would redirect to a fake Twitter account, and even vandalized his South Florida home and dental office. *See* Green, *supra* note 63; Dewey, *supra* note 12.

64. *See* Duggan, *supra* note 52, at 13. The same report also indicates that persons aged 18–24, and African-Americans and Latinos generally, are more likely to face harassment than their peers.

65. *See* McVeigh, *supra* note 9.

66. *See id.*

67. *See id.*

attacks, and suicidal thoughts.[68] In a 2010 U.K. survey jointly conducted by the Network for Surviving Stalking and the National Centre for Cyberstalking Research, a third of respondents indicated that they suffered clinical Post-Traumatic Stress Disorder (PTSD) as a result of experiencing cyberstalking.[69] In a 2012 Australian research study, 84 percent of participants also reported depression, sleeplessness, weight loss, anxiety, panic attacks, and other symptoms of PTSD.[70] In addition, victims of severe cyberharassment and cyberstalking may fear for their safety or the safety of their families, resulting in some being driven from their homes.[71] In response, some victims of cyberharassment limit their online interactions to avoid harassment, limit their offline behavior to prevent perpetrators from obtaining more information about them for use in future incidents, or limit their offline behavior, so as to avoid subsequent offline harassment that stems from their online harassment.[72] For example, some victims do not attend class to avoid having their whereabouts posted online, while other victims carry weapons out of fear of offline attacks.[73]

Given the prevalence of cyberharassment, the ubiquitous nature of the Internet across the globe,[74] and the unique challenges

---

68. *See* Julie Dare, *Cyberharassment and Online Defamation: A Default Form of Regulations*?, 11 TRANSFORMATIONS, 2005, http://www.transformationsjournal.org/journal/issue_11/article_04.shtml; DANIELLE KEATS CITRON, HATE CRIMES IN CYBER SPACE 10–20 (2014).

69. McVeigh, *supra* note 9.

70. DELANIE WOODLOCK, TECHNOLOGY-FACILITATED STALKING: FINDINGS AND RESOURCES FROM THE SMARTSAFE PROJECT (2013), http://www.smartsafe.org.au/sites/default/files/SmartSafe-Findings-Booklet.pdf.

71. Aside from Zoey Quinn, who was driven from her home due to fear from online threats, another female game developer, Brianna Wu, and video game critic, Anita Sarkeesian, similarly were both driven from their homes due to threats against their lives and against their family members. *See* Elise, *supra* note 3; Dewey, *supra* note 2; Kaplan, *supra* note 6.

72. Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 385 (2009).

73. *See id.* at 382, 385.

74. Respectively, 87.9% of the North American population and 73.2% of the Oceania population use the Internet. *Internet Usage Statistics: The Internet Big Picture*, INTERNET WORLD STATS (Nov. 30, 2015), http://www.internetworldstats.com/stats.htm [hereinafter *Internet Usage Statistics*]. Internet usage has grown by over 7,231% in Africa, over 1,319% in Asia, over 3,649% in the Middle East, and over 1,808% in South America between 2000 and 2015. *Id.*

that people face in dealing with cyberharassment, it is crucial that current laws specifically address online harassment as opposed to general harassment. Many Internet users are victims of various forms of cyberharassment. Cyberharassment also has profound effects on its victims, which, in many ways, are more complex than the effects of offline harassment due to the pervasiveness of the Internet and the persistence of data posted on the Internet.[75] Clear and concise laws relating to cyberharassment are thus necessary to ensure that victims have recourse beyond hiding in or fleeing their homes.

II. EXISTING CYBERHARASSMENT AND CYBERSTALKING LAWS ACROSS THE GLOBE

Determining standards for handling cybercrimes can be a difficult endeavor when laws relating to such crimes vary greatly both domestically and internationally. There can be differences in how the crime itself is defined, how standards of intent are used to analyze the perpetrator's actions, which standards are used to analyze the victim's harm, and the types of punishments allocated to those who commit the crime.[76] Creating a unified framework through which to analyze cyberharassment and cyberstalking cases necessarily involves reconciling these different laws. This Part will examine three U.S. federal laws (the ICA, the CA, and the ISPPA) that generally regulate interstate communications and combat cyberharassment and cyberstalking. These federal laws will provide a survey of how U.S. state laws differ in the ways they address (or do not address) particular forms of cyberharassment and cyberstalking. This Part will also analyze the Convention on Cybercrime and Canadian and Australian federal and provincial laws and the challenges associated with enacting cyberharassment and cyberstalking legislation that does not conflict with First Amendment rights and Australia's sentencing structures. These examples can inform how the United States can successfully amend its federal and state laws to address these issues with current laws.

---

75. *See* Merritt Baer, *"Cyberstalking and the Internet Landscape We Have Constructed*,*"* 15 VA. J.L. & TECH. 153, 154–58 (2010); Traci Pedersen, *Cyberstalking Worse Than Stalking?*, PSYCHCENTRAL (Jan. 25, 2015), http://psychcentral.com/news/2015/01/25/cyberstalking-worse-than-stalking/80350.html.

76. *State Legislation*, *supra* note 27.

A. Defining Cyberharassment and Cyberstalking in the United States

The United States uses multiple federal statutes to address a limited subset of cyberharassment and cyberstalking crimes. Many states also have their own laws that cover various subsets of cyberharassment and cyberstalking crimes. This Part will first discuss U.S. federal laws and what those laws do or do not cover. This Part will then address U.S. state laws, what they cover, and how they vary.

1. Federal Laws

The U.S. federal government relies on several laws to prosecute certain forms of cyberharassment.[77] One such law is the ICA.[78] The ICA primarily intends to prohibit intentional extortion across state lines, including threats of harm sent to others over the Internet and threats generally sent with the intent to extort.[79] The scope of the law, however, is limited to extortion specifically and does not focus on intentional injury to others in a general sense.[80] Further, the ICA, and many other statutes that reference threats specifically, only cover true threats (also known as "credible threats").[81] In a nutshell, a "true threat" is a threat that, by its nature, would cause a reasonable person to reasonably fear that the threat will be carried out (even if the person making the threat does not actually intend to carry out the threat).[82] True threat standards can make prosecution of threats over the Internet (especially anonymous threats) particularly difficult, as it is impossible for a victim to know for certain

77. *See* Baer, *supra* note 75, at 154–58; Naomi Harlin Goodno, *Cyberstalking, A New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 MO. L. REV. 125, 148 (2007); Fukuchi, *supra* note 25, at 299.

78. Elonis v. United States, 135 S. Ct. 2001 (2015). The ICA does not specifically refer to the Internet or online behavior but makes illegal all communications sent "in interstate or foreign commerce" that contains a threat to kidnap or injure another person. *See* 18 U.S.C. § 875(c) (2016).

79. The ICA also falls under the Extortion and Threats chapter of the Title 18 statute, further indicating that the law is intended to deal with extortion and related threats, above all else. A subsequent attempt to amend the statute to include conduct performed "with the intent to coerce, intimidate, harass, or cause substantial emotional distress . . . using electronic means" ultimately failed. *See* H.R. Res. 1966, 111th Cong. (2009).

80. *See* United States v. Cooper, 523 F.2d 8 (6th Cir. 1975).

81. Goodno, *supra* note 77, at 148; *see also* Zimmerman, *supra* note 5.

82. *See generally* Zimmerman, *supra* note 5; Goodno, *supra* note 77, at 148.

whether an anonymous perpetrator has the means to carry out a threat until the perpetrator is identified and located.[83] Thus, there are numerous forms of harassment that fall outside the language of the law, including threats that do not fulfill a true threat standard, defamation,[84] and the release of personal information without consent.[85] Further, by the time an investigation reveals the identity and location of a perpetrator, damage to the victim (e.g., fear instilled in the victim, financial loss caused by investigating the message, or other such losses) would have already occurred.[86]

Additionally, the requisite intent of perpetrators under the ICA has historically been ambiguous, at best.[87] Three possible standards of intent for the ICA include general intent (i.e., that the accused intended to send communications that a reasonable person would find threatening), recklessness (i.e., that the accused did not intend to threaten another person but acted in such an egregious manner that he or she should have known that his or her communications would be considered threatening), and specific intent (i.e., the accused intended to threaten another person though his or her communications).[88]

---

83. *See* Baer, *supra* note 75, at 154–58; Goodno, *supra* note 77, at 135–36.

84. While the statute does allow perpetrators to be prosecuted if they send *threats* to damage the reputation of another *with the intent to extort*, it does not include language to prosecute perpetrators if they carry out the threat and publish defamatory statements. 18. U.S.C. § 875(d) (2016) (emphasis added).

85. To their credit, the U.S. Supreme Court and several lower courts have stretched the meaning of the law to attempt to fit threats and threatening language, whether or not it is extortionist in nature. For example, in *Elonis*, the defendant posted threatening language on his Facebook page, but he arguably did not intend to extort the parties that he wrote about. *See* Elonis v. United States, 135 S. Ct. 2001 (2015). 2001. Without a threat of some sort, however, it is difficult for any court to reason that the harassment in question falls under the confines of the statute.

86. Goodno, *supra* note 77, at 135–36.

87. Unfortunately, the legislative history of the ICA is as ambiguous as the language of the statute itself. Scholars disagree as to whether amendments to the ICA, which included new technologies and types of threats over the years, removed the requirement of a subjective intent to threaten, and whether a need to specify objective intent still remains. *See* Megan Chester, *Lost in Translation: The Case for the Addition of a Directness Test in Online True Threat Analysis*, 23 COMMLAW CONSPECTUS 395, 404–05 (2015).

88. Michael Pierce, *Prosecuting Online Threats After* Elonis, 110 NW. U. L. REV. ONLINE 51, 53–57 (2015).

Prior to 2015, most circuit courts interpreted the ICA to include a general intent standard.[89] In 2015, however, the U.S. Supreme Court ruled in *Elonis v. United States* that some criminal intent on the part of the defendant is inherent in criminal statutes (i.e., that, in the absence of a specified intent within the language of a statute, a defendant's intent when acting in a criminal manner must carry some weight).[90] In *Elonis*, the defendant's wife obtained a protection-from-abuse order against him.[91] Subsequent to receiving the order, the defendant posted a message on Facebook asking whether the protection-from-abuse order would be able to stop a bullet.[92] In that same post, the defendant also threatened the authorities by stating that he had enough explosives to defend himself against the state police if his wife tried to enforce the order.[93] The defendant continued to write similar posts about his wife and other parties.[94]

---

89. *See id.* at 412.

90. *See Elonis*, 135 S. Ct. at 2012.

91. *See id.* at 2006.

92. The defendant's message read: "Fold up your [protection-from-abuse order] and put it in your pocket/Is it thick enough to stop a bullet?" *Id.* at 2006.

93. The defendant's post read:

> Try to enforce an Order/ that was improperly granted in the first place/Me thinks the Judge needs an education/on true threat jurisprudence/And prison time'll add zeros to my settlement. . . . /And if worse comes to worse/I've got enough explosives/to take care of the State Police and the Sheriff's Department.

Id. at 2006.

94. Elonis also posted: "That's it, I've had enough/I'm checking out and making a name for myself/Enough elementary schools in a ten mile radius/to initiate the most heinous school shooting ever imagined/And hell hath no fury like a crazy man in a Kindergarten class/The only question is . . . which one?" *Id.* at 2006–07. In reference to a female FBI agent, Elonis wrote:

> You know your s***'s ridiculous/when you have the FBI knockin' at yo' door/Little Agent lady stood so close/Took all the strength I had not to turn the b**** ghost/Pull my knife, flick my wrist, and slit her throat/Leave her bleedin' from her jugular in the arms of her partner/[Laughter]/. . . . Cause little did y'all know, I was strapped wit' a bomb/Why did you think it took me so long to get dressed with no shoes on?/I was just waitin' for y'all to handcuff me and pat me down/Touch the detonator in my pocket and we're all

The U.S. Supreme Court determined that general intent cannot be inferred from criminal statutes that do not explicitly specify an intent standard, as "wrongdoing must be conscious to be criminal," and . . . a defendant must be 'blameworthy in mind' before he can be found guilty."[95] Said another way, the U.S. Supreme Court ruled that, in the absence of a particular intent standard being enumerated in a criminal statute, a defendant must have conscious intent of some manner to commit a criminal act. The U.S. Supreme Court, however, failed to address what criminal intent can and should be used in such statutes (or, specifically, what criminal intent should be used in evaluating defendants' communications under the ICA).[96] Thus, rather than confirming which intent standard can apply to the ICA, the U.S. Supreme Court ruled that one possible intent standard was inapplicable and that it need not decide yet which standards of intent can be applied to the provisions of the ICA.[97] It remains unclear (both to prosecutors and defendants) what sort of intent is necessary to violate the statute.

Two other U.S. federal laws commonly used in cyberharassment and cyberstalking cases include the CA[98] and the ISPPA.[99] The CA covers obscene and harassing communications, and

---

> goin'/[BOOM!]/Are all the pieces comin' together?/S***, I'm just a crazy sociopath. . . .

Id. at 2006–07.

95. *Id.* at 2003, 2012–13.

96. *See id.*

97. Pierce, *supra* note 88, at 59. While potentially frustrating to future litigants, the U.S. Supreme Court's refusal to discuss the merits of the recklessness and specific intent standards is not without its own precedent. Courts often attempt to refrain from ruling on matters that can still be determined through the standard democratic procedures and which are outside the scope of the case at hand. *See* Joseph Russomanno, *Facebook Threats: The Missed Opportunities of* Elonis v. United States, 21 COMM. L. & POL'Y 1, 10–16 (2016).

98. 47 U.S.C.S. § 223 (2016). While originally drafted to handle telephone communications, the statute was amended to include email communication in 2006. *See* Goodno, *supra* note 77, at 148. The statute now prohibits anonymously using a telecommunications device with the intent to abuse, threaten, or harass a specific person or repeatedly communicating with a specific person solely to harass that person. *See* 47 U.S.C.S. § 223(a)(1)(C), (E).

99. 18 U.S.C.S. § 2261A (2016); *see also* Fukuchi, *supra* note 25, at 299. Another law originally dealing with offline behavior, the ISPPA was amended in 2000 and subsequently was found to include interstate conduct performed over the Internet. *See* Fukuchi, *supra* note 25, at 299; United States v. Bowker, 372 F.3d 365, 388 (6th Cir. 2004).

thus, unlike the ICA, covers more than merely credible threats.[100] The CA specifies an intent requirement of specific intent.[101] In U.S. legal discourse, "specific intent" is generally defined as a defendant's actual intent to perform some act, wishing for an expected consequence of the act to occur.[102] Unlike the ICA, the CA requires anonymous communications[103] and for the communications to be sent to a particular person.[104] The CA, therefore, does not cover instances of cyberharassment or cyberstalking that do not involve direct communication with a victim (such as posting private information on a webpage) or instances of cyberharassment or cyberstalking where the victim knows the perpetrator. The ISPPA regulates stalking over state lines and can be used to prosecute some forms of cyberstalking that involve intimidating surveillance (including conduct that causes victims to fear for their safety, to face substantive emotional distress).[105] The ISPPA similarly requires the perpetrator to act with specific intent.[106] Specifically, the accused must have an "intent to kill, injure, harass, intimidate, or place [the victim] under surveillance with intent to kill, injure, harass, or intimidate another person."[107] It can, however, be difficult to prove the intent of a defendant when the defendant harasses a victim online and out of the purview of the victim. For example, Internet conduct is generally divorced from body language, a vocal tone, or other factors that could indicate what a person meant when he or she made a statement, or took an action, online. The more difficulty a prosecutor or victim has in determining these factors, the more difficulty a prosecutor or victim will have in proving that the defendant had any particular intent in saying a particular statement to the victim or performing other actions against the victim. Thus, the extent to which federal laws can

100. 47 U.S.C.S. § 223.

101. *Id.*

102. *See Specific Intent*, CORNELL U. L. SCH., https://www.law.cornell.edu/wex/specific_intent (last visited Sept. 1, 2016). For example, a defendant acts with specific intent when the defendant harasses a victim with the intent to cause some effect on the victim (e.g., to harass or cause fear in the victim). *See* Fukuchi, *supra* note 25, at 306.

103. *See* 47 U.S.C.S. § 223(a)(1)(A); Goodno, *supra* note 77, at 148.

104. *See* Goodno, *supra* note 77, at 148.

105. 18 U.S.C.S. § 2261A (2016); *see also* Fukuchi, *supra* note 25, at 299.

106. 18 U.S.C.S. § 2261A.

107. *Id.*

address many forms of cyberharassment and cyberstalking remains limited.[108]

2. State Laws

State laws can sometimes fill in the gaps formed by federal law but are inconsistent in doing so due to varying definitions of cyberharassment and cyberstalking by state legislatures.[109] Some states passed laws to specifically address online harassment, while others amended their preexisting harassment laws to include online activity.[110] Massachusetts, as an example, defines cyberharassment as a felony offense and requires a "pattern of conduct" (e.g., at least three incidents) directed at a specific person that would cause a reasonable person "substantial emotional distress"; Massachusetts' cyberharassment statute, however, does not actually reference the Internet or computer communications.[111] Under California's misdemeanor statute, repeated and annoying or harassing calls with another person is

---

108. There is growing momentum to pass laws relating to cyberbullying against minors. Though it failed, the findings of the Megan Meier Cyberbullying Prevention Act show that the law was brought to the U.S. Congress due to harassment of minors specifically. *See* H.R. Res. 1966, 111th Cong. (2009). Another bill (that also did not pass) was brought to the U.S. Congress in 2011 after Tyler Clementi, a homosexual student, was cyberbullied by his roommate, who recorded Clementi kissing a male student without Clementi's knowledge and streamed the webcam feed so that other students could watch. *See* S.R. 540, 112th Cong. (2011); Ian Parker, *The Story of a Suicide*, NEW YORKER (Feb. 6, 2012), http://www.newyorker.com/magazine/2012/02/06/the-story-of-a-suicide. Cyberbullying laws, however, would not help adult victims such as Zoe Quinn.

109. Fukuchi, *supra* note 25, at 299; *see also* Goodno, *supra* note 77, at 140–47.

110. Examples of state statutes that specifically address online harassment or stalking include: ARK. CODE ANN. § 5-41-108(a) (2016); LA. STAT. ANN. § 14:40.3 (2016); MD. CODE ANN., CRIM. LAW. § 3-805 (LexisNexis 2016); MICH. COMP. LAWS SERV. § 750.411s (LexisNexis 2016); N.C. GEN. STAT. ANN. §14-196.3 (2016); VA. CODE ANN. § 18.2-152.7:1 (2016); W. VA. CODE ANN. § 61-3C-14a (LexisNexis 2016). Examples of state statutes that include electronic and other communications are: CAL. PENAL CODE § 653m (Deering 2016); MASS. ANN. LAWS ch. 265, § 43A(a) (LexisNexis 2016); N.H. REV. STAT. ANN. § 644:4 (LexisNexis 2016); N.Y. PENAL LAW § 240.30 (LexisNexis 2016); OHIO REV. CODE ANN. § 2917.21 (LexisNexis 2016); 18 PA. CONS. STAT. § 2709 (LexisNexis 2016); TEX. PENAL CODE ANN. § 42.07 (West 2015).

111. MASS. ANN. LAWS ch. 265, § 43A(a); *see also* Commonwealth v. Welch, 444 Mass. 80, 89 (2005); Commonwealth v. Walters, 472 Mass. 680 (2015).

criminalized, regardless of whether or not the victim experienced emotional distress or fear.[112] The statute was amended in 1998 to include electronic communications, but it was not otherwise updated to address online-specific concerns, such as anonymity, disseminating private information to persons other than the victim, and other such issues. California's felony crime requires that a person receive a threat suggesting an imminent and specific threat to the person's safety, but, similar to the misdemeanor statute, it does not address online-specific concerns that can arise in cyberharassment and cyberstalking incidents.[113]

Currently, only a handful of states have cyberharassment and cyberstalking statutes that specifically address online communications. The Arkansas Code, for example, defines cyberharassment as a misdemeanor offense that criminalizes the sending of a computerized message that contains the threat of physical injury or lewd or obscene language, which "frighten[s], intimidate[s], threaten[s], abuse[s], or harass[es] another person."[114] The Arkansas Code, however, still only criminalizes communications sent to a victim for the purpose of threatening physical injury or conveying profane language, of which the former constitutes a threat of offline harm. The statute thus does not cover threats that involve online-specific activity (such as releasing private information, hacking, and other such actions). Michigan's Penal Code provides one of the few examples of a state cyberharassment and cyberstalking law that addresses online-specific consequences and behaviors. Under Michigan's Penal Code, a perpetrator commits a felony when he or she has reason to believe that the posting of an online message will cause others to send unwanted messages to the victim and would cause the victim emotional distress.[115] In addition to online-specific concerns regarding communications and the nature of those communications, only some states criminalize anonymous commu-

112. CAL. PENAL CODE § 653m(b).
113. CAL. PENAL CODE § 422 (Deering 2016).
114. ARK. CODE ANN. § 5-41-108(a).
115. MICH. COMP. LAWS SERV. § 750.411s.

nications within their cyberharassment and cyberstalking statutes.[116] Other states fail to have any law addressing online harassment.[117] Thus, many states include very different elements in their cyberharassment and cyberstalking statutes, or fail to address online-specific issues in their statutes. As a result, the clear lack of consensus between the states and the federal government in how to define various elements of cyberharassment and cyberstalking crimes leads to vast inconsistencies in whether victims can seek a legal remedy in different jurisdictions throughout the United States.[118]

Criminal intent standards can also vary widely based on state jurisdiction.[119] While Arkansas' definition of cyberharassment may in some ways be fairly broad (in the sense that Arkansas' definition of cyberharassment and cyberstalking criminalizes a wider variety of activity), Arkansas requires specific intent on the part of the perpetrator to cause harm to another.[120] Massachusetts does not require specific intent on the part of the perpetrator to cause a particular harm to another (i.e., a person in Massachusetts need not intend to harass or threaten the victim),

---

116. States with laws specifying that the accused may be anonymous include: Alabama (ALA. CODE § 13A-11-8(b)(1) (LexisNexis 2016)); Arizona (ARIZ. REV. STAT. § 13-2912 (LexisNexis 2016)); Colorado (COLO. REV. STAT. § 18-9-111 (2016); Hawaii (HAW. REV. STAT. ANN. § 711-1106 (LexisNexis 2016)); and Kentucky (KY. REV. STAT. ANN. § 525.080 (LexisNexis 2017)). Such clauses can be helpful, as they allow for victims to reasonably perceive a threat, even if they do not know the accused and, therefore, cannot know whether the accused was likely or able to follow through on the threat. Most states, however, do not have such clauses including anonymity in their statutes. *See State Legislation*, *supra* note 27.

117. *State Legislation*, *supra* note 27. Many of these states do have statutes addressing cyberbullying, including Idaho and Kansas. *See* IDAHO CODE § 18-917A (2016); KAN. STAT. ANN. § 72-8256 (LexisNexis 2017). As noted above, however, cyberbullying generally is specific to minors and, therefore, generally cannot be applied to harassment committed by adults against other adults.

118. *See* Goodno, *supra* note 77, at 158–97; Fukuchi, *supra* note 25.

119. *See* Goodno, *supra* note 77, at 158–97.

120. *See* ARK. CODE ANN. § 5-41-108(a) (2016) ("A person commits the offense [cyberharassment] . . . if, with the purpose to . . . harass another person, the person sends a message."); *see also* MASS. ANN. LAWS ch. 265, § 43A(a) (LexisNexis 2016). Malice is defined by "wilful [sic] doing of . . . unlawful acts, without justification or mitigation," such that "any reasonably prudent person would have foreseen the actual harm that resulted." Commonwealth v. O'Neil, 67 Mass. App. Ct. 284 (2006). In *O'Neil*, the court noted the unlikelihood that "the Legislature would have expected a specific intent to alarm or harm the victim under these circumstances." O'Neil, 67 Mass. App. Ct. at 293.

but it does require the perpetrator to have maliciously acted in a way that caused a reasonable person to be distressed.[121] California law requires a perpetrator to make a threat "with the specific intent that the statement . . . be taken as a threat" and also uses an objective standard from the victim's perspective to determine whether it was reasonable for the person to have feared an imminent threat.[122] In Michigan, there is an even more varied mix of standards for either the perpetrator or the victim.[123] For example, a perpetrator is required to have specific intent to cause conduct that would harass the victim, but he need not have specific intent in causing separate unconsented contact that would cause the victim emotional distress.[124] Further, a prosecutor must also show that a victim both subjectively suffered emotional distress, by feeling frightened or harassed from conduct that arises from the perpetrator's message, and that, objectively, a reasonable person would have suffered emotional distress and would have felt frightened or harassed.[125] Various other states have differing intent standards for the perpetrator and use different standards for the victim's perspective.[126] Different intent standards for cyberharassment and cyberstalking, coupled with widely varying definitions of the crimes themselves, can affect the degree to which a victim or a prosecutor can reasonably maintain a case against a perpetrator, who may be located hundreds of miles away.[127]

---

121. *O'Neil*, 67 Mass. App. Ct. at 293.

122. CAL. PENAL CODE § 422 (Deering 2016). The California statute calls for the victim to reasonably fear for their life due to the "unconditional, immediate, and specific" nature of the threat. *Id.* § 422(a).

123. MICH. COMP. LAWS SERV. § 750.411s (LexisNexis 2016).

124. Section 750.411s(a) of the Michigan code requires that the accused "know[] *or should have known*" that the posting could cause a particular effect on other perpetrators. *Id.* § 750.411s(a). Section 750.411s(b) of the Michigan code, on the other hand, requires the specific intent of causing other perpetrators to make the victim feel threatened or otherwise harassed. *See id.* § 750.411s(b).

125. *Id.*

126. As one example, New York requires an intent to offend or harass, but it does not require an intent to cause emotional distress or other harms and does not include a standard for analyzing whether or not the victim was harmed. N.Y. PENAL LAW § 240.30 (LexisNexis 2016).

127. For example, it may be less reasonable to argue that a defendant intended to fulfill a threat to harm the victim if the perpetrator happens to live thousands of miles away than it would be if the perpetrator lived next door.

B. Defining Cyberharassment Internationally

Outside the United States, definitions of cyberharassment can also vary greatly. Legal definitions of cyberharassment and cyberstalking can vary just as greatly between nations as they can within the United States specifically. This section will examine the scope of Canadian law (including the Canadian Criminal Code, Nova Scotia's CSA, and Ontario's civil tort law) and recent amendments to Australia's federal Criminal Code Act of 1995 to analyze how these countries define cyberharassment and cyberstalking in comparison to the United States. This section will also analyze the Council of Europe's Convention on Cybercrime (COC) (the leading international treaty specifically dealing with online crimes) and will note its shortcomings with respect to the scope treaty as it currently exists and its power (or lack thereof) to affect the laws of its member states.

1. Canada

Much like the United States, Canada has a general federal criminal harassment statute that can be used to prosecute persons who harass others online.[128] Section 264 of the Canadian Criminal Code criminalizes conduct that causes another person to reasonably fear for their safety, including following that person around, repeatedly communicating with that person, watching that person's home or work place, or threatening that person in some manner.[129] While the Canadian Criminal Code does not specifically address online communication, it has been used to prosecute individuals who have committed harassment[130] using online tactics, such as sexual harassment via texting, threatening to call the police on another, placing false information about a victim on websites, tampering with a victim's online accounts, sending rape threats over the Internet, and various other online behavior.[131] Unlike the ICA of the United States, the Canadian

128. Criminal Code, R.S.C. 1985, c C-46, s 264(1) (Can.).

129. *Id.* s 264(1), (2)(a)–(d).

130. The Canadian statute does not require harassment to comprise repeated acts. While the statute's definition of "harassed" includes many components, including repeated acts, the components are intended to be taken as independent, individual synonyms of harassment, not as components that cumulatively define harassment. *See* R. v. Kordrostami, 2000 CarswellOnt 554, paras. 6–7 (Can. Ont. C.A.) (WL).

131. R. v. A. (B.L.), 2015 CanLII 203, paras. 9–14 (BCPC) (Can.). Other behavior the defendant in *R. v. A.* admitted to committing, and which was subject

Criminal Code specifies the requisite intent of the accused: the accused act "knowing that another person is harassed or recklessly as to whether the other person is harassed."[132] In other words, a perpetrator must act with the intent that his or her conduct is harassing the other person or must harass the other person in such a manner that it would be unreasonable for the perpetrator not to know that his or her conduct is harassing in nature.[133] The Canadian Criminal Code also requires that, regardless of the nature of the accused's actions, the victim must reasonably fear for his safety.[134] Thus, the Canadian Criminal Code allows for a conviction if the perpetrator acts with either specific intent or reckless intent. Further, the Canadian Criminal Code uses both an objective and subjective standard to examine the effect of the perpetrator's actions on the victim. Specifically, the Canadian Criminal Code requires the victim to subjectively fear for his or her safety and requires that fear to be objectively reasonable.

Various provinces in Canada also have passed statutes that have been used to prosecute cyberharassment and cyberstalking. Following the suicide of a student who endured cyberharassment, Nova Scotia passed the CSA,[135] which was the first law passed in Canada that attempted to protect victims from online harassment.[136] The CSA allows two avenues for prosecuting children for cyberbullying (i.e., cyberharassment and cyberstalking performed between two minors).[137] Under the CSA, children who

---

to prosecution under the statute, included disrupting a woman's internet service after she refused to send the defendant sexual photos, posting an advertisement on Craigslist with the victim's real name indicating that she wanted sex, and impersonating another victim on Skype to obtain sensitive information about her from her friends. *Id.*

132. R.S.C. 1985, c C-46, s 264(1) (Can.).

133. *See* Karen D. Levin, *La Cyberintimidation: Analyse Juridique*, 8 CAN. J. L. & TECH. 65, 69 (2010).

134. R.S.C. 1985, c C-46, s 264(1); *see also* Levin, *supra* note 133.

135. Hannah E.Y. Choo, *Why We Are Still Searching for Solutions to Cyberbullying: An Analysis of the North American Responses to Cyberbullying Under the Theory of Systemic Desensitization*, 66 U.N.B.L.J. 52, 59 (2015).

136. Brett Ruskin, *Court Strikes Down Anti-Cyberbullying Law Created After Rehtaeh Parsons's Death*, CBC NEWS (Dec. 11, 2015, 11:45 AM), http://www.cbc.ca/news/canada/nova-scotia/cyberbullying-law-struck-down-1.3360612.

137. *See* Cyber-safety Act, S.N.S. 2013, c 2, s 3(1)(b) (Can.). The Cyber-safety act was invalidated by *Crouch v. Snell*. *See* Crouch v. Snell, 2015 NSSC 340, para. 141; *see also Cyberbullying/Stalking & Harassment*, *supra* note 39.

intend to cause fear, or even "humiliation," to another child, or who encourage or help another child humiliate or hurt the feelings of another student are liable.[138] A parent could also be culpable for cyberbullying under the CSA merely by failing to prevent their child from engaging in activities that the parent knows would humiliate another child.[139] The law was so broad that it was quickly contested (and invalidated) in Nova Scotia courts for violating Canada's Charter of Rights and Freedoms.[140] Similarly, in 2016, the province of Ontario adopted a civil law tort to prevent persons from publicly distributing "embarrassing private facts."[141] Modeled after a similar tort established in the province of Manitoba,[142] Ontario's Superior Court of Justice held that a person violates a common law duty not to distribute embarrassing private facts about a victim when (1) the person disseminates confidential information; (2) the person shares this information, despite having an obligation to keep the information in confidence; and (3) the information was shared to the detriment of the victim.[143] This common law tort was used against a defendant accused of posting a sex tape of his ex-girlfriend on a pornography website.[144]

2. Australia

Currently, Australia relies on an August 2015 amendment to the Australian Criminal Code Act of 1995 (ACCA) to police cyberharassment and cyberstalking.[145] Multiple components of

---

138. *See* S.N.S. 2013, c 2, s 3(1)(b) ("[C]yberbullying' means any electronic communication . . . that is intended or ought reasonably be expected to cause fear, intimidation, humiliation, distress or other damage or harm to another person's health, emotional well-being, self-esteem or reputation, and includes assisting or encouraging such communication in any way.").

139. *See* S.N.S. 2013, c 2, s 3(2).

140. *Halifax Lawyer to Launch Charter Case Challenge of Cyber-Safety Act*, *supra* note 36.

141. *Cyberbullying and the Law*, MEDIA SMARTS, http://mediasmarts.ca/digital-media-literacy/digital-issues/cyberbulling/cyberbullying-law (last visited Jan. 17, 2017).

142. Manitoba was the first (and until 2016, the only) province in Canada to have a tort covering the distribution of private images. *See* Jane Doe 464533 v. N.D., 2016 ONSC 541, para. 18.

143. *Id.* para. 21.

144. *Id.* para. 8.

145. *See Criminal Code Act 1995* (Cth) ch 10 div 474 sub-div C (Austl.).

the ACCA can be used to prosecute different levels of harassment, such as §§ 474.14–474.17, which specifically relate to electronic communications.[146] ACCA § 474.14 criminalizes one who intentionally connects to the Internet to commit an offense against an Australian law or against a foreign law.[147] ACCA § 474.14 does not require proof that a victim of the offense felt or reasonably could have felt a particular way after the offense was committed (in other words, it does not impose any standards on the perspective of the victim); it primarily focuses on the specific intent of the accused.[148] ACCA § 474.15 criminalizes the use of the Internet to send a death threat with the intent that the recipient of the threat will fear that the threat will be carried out.[149] As with ACCA § 474.14, ACCA § 474.15 requires specific intent on the part of the accused, but it does not specify a particular intent or standard in analyzing the perspective of the victim.[150] ACCA § 474.16 criminalizes sending online communications with the intent that the recipient will believe that a dangerous substance or object has been, or will be, left in a place (i.e., a threat that a bomb has been left in a public place).[151] Similar to ACCA § 474.14 and ACCA § 474.15, ACCA § 474.16 requires specific intent on the part of the accused, but it does not require a particular state of mind for the victim.[152] Lastly, ACCA § 474.17 criminalizes sending internet messages in a manner that reasonable people would interpret as being harassing, menacing, or offensive.[153] Unlike §§ 474.14–474.16 of the ACCA, ACCA § 474.17 does not require specific intent on the part of the accused but does require using an objective standard to assess the perspective of the victim.[154]

There are many benefits to the Australian cyberharassment and cyberstalking section of the ACCA. Particularly due to the flexibility that ACCA § 474.17 offers (in terms of conduct that may fall under the purview of the statute), the ACCA does not

146. *See id.*

147. *Id.* s 474.14. This section of the code does not require proof that a victim of that offense suffers any particular consequences (other than those specified by the law); it primarily focuses on the intent of the accused.

148. *Id.*

149. *Id.* s 474.15.

150. *Id.*

151. *Id.* s 474.16.

152. *Id.*

153. *Id.* s 474.17.

154. *Id.*

merely criminalize true threats or stalking, as is the case in many U.S. jurisdictions, but can also be used (and has been used) to prosecute defamation-related harassment suits[155] and posting of offensive messages on social networks.[156] Thus, many different aspects of cyberharassment and cyberstalking can be covered under the statute (rather than only threats or conduct that causes substantial emotional distress, as is present in much of U.S. cyberharassment and cyberstalking law). Further, ACCA § 474.14, which criminalizes using the Internet to violate Australian and foreign laws alike, may further extend the scope of Australia's ACCA to cover cyberharassment that violates the laws of other countries or of states and territories of Australia that are not necessarily embodied in the ACCA itself.[157] Specifically, ACCA § 474.14 states:

> A person is guilty of an offence if: (a) the person: (i) connects equipment to a telecommunications network; and (ii) intends by this to commit, or to facilitate the commission of, an offense . . . and (b) the offense is: (i) a serious offense against a law of the Commonwealth . . . or (ii) a serious offence against a foreign law.[158]

---

155. *Cullen v White* [2003] WASC 153 (Austl.). In *Cullen*, the defendant made several websites impersonating the plaintiff and insinuating that the plaintiff was a pedophile, a fraud, and a dangerous felon. *Id.* paras. 7–8. The court ruled in favor of the plaintiff and awarded punitive damages. *See id.*

156. *R v Hampson* [2011] QCA 132 (Austl.). In *Hampson*, the defendant posted Facebook messages on the wall of a deceased child, including a picture of the child with the caption: "WOOT IM DEAD." *Id.* para. 12. The defendant also posted a picture of the child Photoshopped into a photograph of a woodchipper with the caption: "This woodchipper can mince up any dead corpse or your money back guarantee." *Id.*

157. *See* Gregor Urbas, *Why Julian Assange May Have a Case to Answer in Australia, Despite What the AFP Says (or, Why Julia Gillard Might be Right)* (ANU Coll. of Law, Res. Paper No. 11-04, 2011), http://ssrn.com/abstract=1733666. While not specifically referring to cyberharassment, the paper applies the ACCA to Julian Assange and the Wikileaks scandal, which involved the release of hundreds of classified documents, noting that "conduct that gives rise to a serious offense against foreign law must also be such as to give rise to a serious offence against a law of Australia, had the conduct occurred in Australia." *Id.* at 7. The paper goes on to note, therefore, that if the leaks had at any point occurred in Australia, the alleged violators of U.S. law could also be found culpable under the ACCA § 474.14. *Id.*

158. *Criminal Code Act 1995* (Cth) ch 10 div 474 sub-div C s 474.14(1).

Based on the language of the statute, the law allows Australian courts to prosecute Australians who harass others extraterritorially (whether those Australians are acting within Australia or acting within another jurisdiction at the time), so long as their behavior violated both the laws of the country in which the victim resides and some Australian law.[159] As one example, had any of Zoe Quinn's perpetrators been Australian citizens who attacked her while visiting the United States (i.e., while acting outside of Australia),[160] it is possible that they could have still been prosecuted in Australia for their harassment (i.e., for violating a U.S. cyberharassment or cyberstalking law, so long as the perpetrator's conduct would have also been a serious offense in Australia if performed in Australia).[161] Further, had any of Quinn's perpetrators used the internet while present in Australia in a manner that was meant to encourage U.S. citizens to commit cyberharassment or cyberstalking crimes that would violate U.S. or Australian law, the ACCA could also be used to prosecute that perpetrator.[162] Said another way, in theory, the ACCA allows Australia to bring criminal charges against people whose online activities violate serious cyberharassment or cyberstalking laws and prosecute Australian citizens who encourage or help citizens of other nations commit offenses that would violate both their domestic laws and the laws of Australia.

An additional benefit of the ACCA is that portions of the statute do not require any particular intent on the part of the perpetrator or proof that the victim was indeed afraid for his or her life.[163] For example, § 474.17(1) does not require intent on the

159. *See* Urbas, *supra* note 157, at 7.

160. Because it is a federal statute, the ACCA also allows Australian citizens to bring claims against perpetrators in different Australian states. *See Doe v Yahoo!7 Pty Ltd* [2013] QDC 181 (Austl.).

161. The ACCA defines a "serious offence" as an offense punishable for at least five years. *Criminal Code Act 1995* (Cth) ch 10 div 473.1 (Austl.). Further, a serious offence against a foreign law specifically is defined as "an offense against a law of a foreign country constituted by conduct that, if it had occurred in Australia, would have constituted a serious offence against a law of the Commonwealth, State, or Territory." Urbas, *supra* note 157, at 7; *Criminal Code Act 1995* (Cth) ch 10 div 473.1. In other words, assuming there was a state where the person's conduct would result in a five-year sentence in the United States but only a three-year sentence in Australia, the victim would not be able to use the ACCA to prosecute the perpetrator, as the analogous Australian crime would not constitute a "serious offence."

162. Urbas, *supra* note 157, at 7.

163. *Criminal Code Act 1995* (Cth) ch 10 div 474 sub-div C s 474.

part of a perpetrator to harass another; it merely requires evidence that the perpetrator used the Internet in a harassing manner.[164] Similarly, § 474.15 does not require the victim to feel that his or her life was in danger; rather, it necessitates that the perpetrator intended to create that effect.[165] By not requiring proof that a victim suffered a particular consequence of the harassment, the ACCA allows for the prosecution of harassing behavior, even when the victim does not suffer specific harms specified by the legislature. By requiring a particular intent for some crimes and allowing general intent for other crimes, the ACCA allows for both the prosecution of harassing behavior when it is difficult to ascertain the true intent of the accused and protection for defendants who communicate harassing material without realizing the severity of their actions.

3. International Law

The COC is the first, and only, binding international treaty for regulating international cybercrimes.[166] Drafted as a mechanism for defining "a common criminal policy aimed at the protection of society against cybercrime," the COC officially entered into force in 2004 to encourage international cooperation in dealing with online criminal acts that were increasingly becoming a global, rather than merely an intrastate, issue.[167] As of the date of this publication, fifty-one states (including several nonmembers of the Council of Europe, such as the United States, Canada, and Australia) have ratified the COC.[168]

The COC, however, is a largely ineffective mechanism for cyberharassment and cyberstalking victims who are seeking legal recourse from an entity other than their resident state. The COC, for example, calls for the criminalization of nine offenses, including illegal access, illegal interception, data interference,

---

164. *Id.* s 474.17(1).

165. *Id.* s 474.15.

166. *See* Amalie M. Weber, *The Council of Europe's Convention on Cybercrime*, 18 BERKELEY TECH. L.J. 425, 429 (2003); *see also Details of Treaty No. 185*, *supra* note 31; *Budapest Convention and Related Standards*, COUNCIL EUR., http://www.coe.int/en/web/cybercrime/the-budapest-convention (last visited Jan. 17, 2017).

167. *See* Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167 (entered into force July 1, 2004).

168. *See Chart of Signatures and Ratifications of Treaty 185*, COUNCIL EUR., http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=YLI5WLtp (last visited Jan. 17, 2017).

system interference, misuse of devices, computer-related fraud and forgery, dissemination of racist or xenophobic material, dissemination of child pornography, and copyright violations.[169] Many of these offenses are unrelated to harassment or stalking crimes and are thus futile to victims seeking a legal remedy for online harassment. For example, provisions for copyright violations, child pornography, and computer-related fraud crimes share little connection to cyberharassment and cyberstalking crimes. Further, racist and xenophobic materials could potentially be harassing in nature but would only cover a very narrow subset of cyberharassment or cyberstalking offenses (e.g., they would not cover threats unrelated to race or immigration status, defamation, revenge porn, or other forms of online harassment or stalking). Further, as the United States was one of the lead drafters of the COC, many of the provisions suggested mirror those that are already covered by U.S. law.[170] As a result, many of the issues associated with U.S. federal law are further replicated in the COC. Specifically, the COC does not cover all forms of cyberharassment and cyberstalking and is limited to a very narrow subset of cyberharassment and cyberstalking offenses (such as harassment that is specifically racial or xenophobic in nature).

The COC is also overly broad, allowing member states to ratify the treaty without enacting specific legislation that would target particular cyberharassment or cyberstalking activity. As one example, to the extent there are provisions in the COC that are not expressed in existing U.S. legislation, the United States has maintained that the COC is ambiguous enough that existing U.S. law can be implied to cover the crimes specified in the convention (and, consequently, that the United States need not amend its existing laws to further accommodate other cybercrimes).[171] Thus, the COC has not caused meaningful changes to U.S. law, and (in its current state) it is unlikely to spur future amendments to U.S. law. Similarly, with respect to Canada, while the country ratified the COC in July 2015, the portion of the federal Criminal Code used to prosecute cyberharassment

169. *See* Weber, *supra* note 166, at 431.
170. *See id.* at 435–36.
171. *See id.*

and cyberstalking crimes has not been amended since 1993.[172] Considering that U.S. and Canadian cyberharassment and cyberstalking laws have gaps with respect to the types of conduct they cover, if the COC does not require these countries to amend their laws to include additional forms of cyberharassment and cyberstalking, then the COC could not serve as a mechanism for forcing these two nations to fill in those gaps, and therefore allows nations to operate with incomplete cyberharassment and cyberstalking legislation.

III. LESSONS FROM CYBERHARASSMENT AND CYBERSTALKING LAWS ACROSS THE GLOBE

Each jurisdiction has its own definition of cyberharassment and cyberstalking. The United States, Canada, and Australia criminalize widely different forms of cyberharassment and cyberstalking, causing victims to fall through the gaps established by these definitions (e.g., when the victim's experiences do not correlate to the narrow definitions covered by that particular jurisdiction). Existing U.S. law also discourages law enforcement from investigating cyberharassment and cyberstalking crimes due to the costs of investigating these crimes and the relatively low sentences prosecutors are likely to obtain if they successfully prosecute these crimes. In Canada, conflicts between cyberharassment and cyberstalking laws and constitutional rights have slowed the progression and effectiveness of these laws. In Australia, there are problems with the scope of Australian law with respect to which forms of cyberharassment and cyberstalking the laws do (or do not) cover. Australia's laws, however, also offer potential solutions to dealing with interstate actors and creating sentencing structures that make investigation efforts proportionate to the potential punishments of these crimes. This Part will discuss gaps that exist in current U.S., Canadian, and Australian cyberharassment and cyberstalking laws. These gaps exist not only in the ways in which jurisdictions define cyberharassment and the intent standards used to examine defendants' behavior but also in the ways in which the laws punish the ac-

172. *Chart of Signatures and Ratifications of Treaty 185*, *supra* note 168; *see also* GARY P. RODRIGUES, CRANKSHAW'S CRIMINAL CODE OF CANADA: LEGISLATIVE HISTORIES (2016).

cused. This Part will also discuss aspects of Canadian and Australian law that do help cyberstalking and cyberharassment victims, such as clear intent standards and staggered sentencing.

A. Problems with U.S. Cyberharassment Laws

Federal laws of the United States have their fair share of complications that prevent prosecutors from successfully winning cyberharassment cases in court. The ICA, for example, is primarily concerned with extortion[173] rather than general threats or intentional injury to others.[174] Thus, many forms of harassment, such as defamation and intentionally causing distress to others, do not fall under the purview of the statute. Further, the ICA has also been difficult to enforce due to a cloud of uncertainty over what intent is actually required by the statute on the part of the accused.[175] In *Elonis*, the defendant was accused of posting threatening messages on Facebook.[176] Because the ICA did not explicitly provide an intent standard for the defendant, nine U.S. circuit courts decided that threats under the ICA only required proof of general intent of the accused.[177] Therefore, a defendant could be found guilty, so long as the defendant sent communications that could be reasonably construed as a threat.[178] In *Elonis,* the U.S. Supreme Court ruled, however, that a general intent standard for the ICA would "reduce[] culpability on the all-important element of the crime to negligence," a standard that is not typically inferred into criminal statutes that lack an explicit *mens rea.*[179] While the U.S. Supreme Court ruled in *Elonis* that the ICA requires more than general intent, the court declined to determine whether other standards of intent, such as recklessness,[180] would meet the requisite *mens rea*

173. *See* H.R. Res. 1966, 111th Cong. (2009).
174. *See id.*; United States v. Cooper, 523 F.2d 8 (6th Cir. 1975).
175. *See* Elonis v. United States, 135 S. Ct. 2001 (2015).
176. *Id.* at 2006–07.
177. *See id.* at 2018 (Thomas, J., dissenting).
178. *See id.*
179. *Id.* at 2013.
180. Under the Model Penal Code, the *mens rea* of recklessly entails the following:

> A person acts recklessly . . . when he consciously disregards a substantial and unjustifiable risk that the material element [of an offense] exists or will result from his conduct . . . [where] [t]he risk must be of such a nature and degree that .

under § 875(c) of the statute.[181] Though litigants are now aware that merely intending to post content that can be interpreted as a threat is not on its own sufficient to violate § 875(c) of the ICA, litigants and courts have no guidance as to what theory of intent will prevail in such a case. Even if U.S. circuit courts come to an agreement about what kind of intent is required for § 875(c),[182] litigants would need to ask the U.S. Supreme Court to provide further clarification of the statute.[183]

> . . its disregard involves a gross deviation from the standard of conduct that a law-abiding person would observe in the actor's situation.

MODEL PENAL CODE § 2.02(2)(c) (AM. LAW INST., Proposed Official Draft 1962).

181. *Elonis*, 135 S. Ct. at 2017 ("We think that is more than sufficient 'justification'. . . for us [the court] to decline to be the first appellate tribunal" to decide "whether recklessness suffices for liability under Section 875(c)."). While judicial minimalism can, at some level, be understandable when dealing with such a broad and complex area of law, it is not completely unprecedented for justices to discuss, even in the abstract, the complexities of the law as well as ponder what the U.S. Congress could do to address these issues going forward. *See* Russomanno, *supra* note 97, at 15–16. It may be true that it was not the U.S. Supreme Court's place to decide for certain whether or not a reckless standard or a subjective intent standard should prevail in a case such as *Elonis*, but it is nevertheless disappointing that the majority (and to some extent, the dissent) failed to bring attention to the issues that remain in the language of the ICA, and in the landscape of cyberharassment and cyberstalking laws in general, when general intent cannot be used as the standard of intent. By refusing to bring that context into the discussion of the statute and the facts of the case, the court arguably missed an opportunity to encourage the U.S. Congress to further review the effects and scope of the federal laws currently in effect and to consider alternative approaches to dealing with online activity. Such discussions have certainly helped move legislation forward in areas outside of cyberharassment and cyberstalking. *See generally id.*

182. As of the date of publication, no lower court has directly addressed the issue of recklessness post-*Elonis*.

183. *See Elonis*, 135 S. Ct. at 2013 (Alito, J., concurring in part and dissenting in part). For now, the Third Circuit, on remand, has only ruled that the statute "contains both a subjective and objective component," such that prosecutors must prove that a defendant transmitted a communication for the purpose of issuing a threat or knew that the communication would be perceived as a threat and that a reasonable person would view the communication as a threat. *See* United States v. Elonis, 2016 U.S. App. LEXIS 19453, *13 (2016). The court ruled that, since the remand was predicated on a harmless error issue arising from jury instructions, the court need not determine whether recklessness would suffice as the requisite *mens rea* under the statute. *See id.* at *27. The Fourth Circuit, having decided similar cases post-*Elonis*, has similarly ruled

Similar to the ICA, the scope of the CA is also narrowly tailored; many of the provisions in the CA are specifically directed to preventing the transmission of lewd content.[184] Another inherent limitation of the CA is that it requires a person to repeatedly initiate communications with a telecommunications device "solely to harass" a specific person.[185] Specific or "sole" intent in cases of cyberharassment and cyberstalking, however, can be problematic, as it is difficult to provide evidence that a defendant's one and only reason for performing an action was to harass a specific person.[186] Lastly, the CA only applies if the perpetrator does not disclose his identity and communicates with the intent to abuse, threaten, or harass a specific person.[187] In the case of Zoe Quinn, the CA would have allowed law enforcement to charge any of the anonymous harassers who sent rape threats and death threats directly to her, assuming an investigation could uncover the specific person who created the message.[188] The CA, however, would not allow for charges against Gjoni (e.g., a perpetrator she can identify) with respect to his blog posts because his blog posts were not anonymous.[189] Additionally, based on the plain language of the statute, the CA would also not allow

---

that Section 875(c) now requires "'(1) that the defendant knowingly transmitted a communication . . . ; (2) that the defendant subjectively intended the communication as a threat; and (3) that the content of the communication contained a "true threat" to kidnap or injure.'" Shah v. United States, 2016 U.S. Dist. LEXIS 157843, *14–15 (2016) (citing United States v. White, 810 F.3d 212, 220–21 (4th Cir. 2016)). In applying *Elonis* to another case, one state court judge opined that merely adopting general intent for federal criminal statutes that do not specify a *mens rea* would allow for civil standards of care to creep into criminal statutes. People v. Salamon, 2016 N.Y. Misc. LEXIS 4279, *12–28 (2016).

184. *See* 47 U.S.C.S. § 223(a)(1)(A), (B) (2016).

185. *Id.* § 223(a)(1)(E).

186. Fukuchi, *supra* note 25, at 306.

187. 47 U.S.C.S. § 223(a)(1)(C); *see also* Goodno, *supra* note 77.

188. *See* Dimeo v. Max, 433 F. Supp.2d 523 (E.D. Pa. 2006); United States v. Tobin, 552 F.3d 29, 33 (1st Cir. 2009). Note that Quinn would not be able to, say, hold a website or other publisher accountable for displaying the threats. *See Dimeo*, 433 F. Supp.2d at 529–32. Courts have both held that it is important to allow free and uncensored dissemination of information over the Internet and that websites would be facing an onerous burden if they had to immediately deal with every comment from a user that could be considered threatening. *Id.*

189. *See Dimeo*, 433 F. Supp.2d at 531. Similarly, the CA would not have helped convict the defendant in *Elonis*, who did not anonymously post the threats he made about his wife. *See id.*

Quinn to bring any claims against any perpetrators who posted her personal information, defamatory statements, or even death or rape threats, on a website or forum, as such posts would not be communications to a specific person (regardless of whether the perpetrators were identifiable).[190] Thus, the limits of the CA (which is only directed to crimes where a person is directly harassing a person anonymously) prevent many online harassers and stalkers from being prosecuted under this federal law. The ISPAA is not as narrowly tailored as the ISA or the CA, as the ISPAA covers both conduct that causes a victim to fear for his or her safety and causes a victim substantial emotional distress.[191] The ISPAA, however, includes a specific intent standard that can be difficult to prove in cases involving conduct that is wholly online.[192]

Additionally, state laws can vary in their coverage of cyberharassment because of the way they define conduct and intent sufficient for criminalization in their statutes.[193] The inconsistencies between states can greatly affect what kind of legal recourse litigants have across the country.[194] For example, in California and Massachusetts, prosecutors would have to show repeated attempts of harassment to win a cyberharassment suit.[195] Conversely, in Michigan and Arkansas, one incident could suffice.[196] These inconsistencies can cut both ways.[197] For example, a defendant living in one state could publish content online without any notion of where the subjects of the content live within the United States. Additionally, a defendant living in one state and acting against another person in another state could believe that each state generally follows the same definition of cyberharassment or cyberstalking as his or her own. He or she could be just

190. 47 U.S.C.S. § 223(a)(1)(C).

191. 18 U.S.C.S. § 2261A (2016).

192. *Id.*; *see also* Fukuchi, *supra* note 25.

193. *See supra* Part II. *See generally* Goodno, *supra* note 77; *State Legislation*, *supra* note 27; Fukuchi, *supra* note 25.

194. *See generally* Goodno, *supra* note 77; Fukuchi, *supra* note 25.

195. *See* CAL. PENAL CODE § 653m(b) (Deering 2016) (noting that a defendant would be guilty if he or she "[m]akes repeated telephone calls or makes repeated contact by means of an electronic communication device"); Commonwealth v. Robinson, 444 Mass. 102, 109 (2005).

196. *See* ARK. CODE ANN. § 5-41-108(a) (2016) (sends "a" message); MICH. COMP. LAWS SERV. § 750.411s (LexisNexis 2016) ("A person shall not post a message. . . .").

197. *See generally* Goodno, *supra* note 77; *State Legislation*, *supra* note 27.

as surprised to find out that another state has a much more lenient definition of the crime. A person at risk of being accused of cyberharassment or cyberstalking, therefore, would effectively need to have working knowledge of every cyberharassment and cyberstalking law in the country to know for sure whether a post he or she believes is harmless may nonetheless qualify as a criminal offense in a specific state.

Even if these gaps in current U.S. cyberharassment and cyberstalking laws were fixed, however, there would still be a need to incentivize law enforcement to investigate cyberharassment and cyberstalking cases to gather enough facts to prosecute cyberharassers in the first place. As previously noted, U.S. law enforcement may be reluctant to step in and investigate cyberharassment and cyberstalking crimes when the punishment for the crime is not proportional to the scope of the work required to investigate the crime.[198] Because law enforcement may not be trained in investigating sophisticated Internet matters, law enforcement often requires specialized training by personnel (e.g., in federal agencies) who have experience investigating cybercrimes.[199] The cost of such investigations can cost as much as $2,500–$3,500 for individuals and attorneys seeking to perform their own private investigations.[200] This cost could be even greater for law enforcement agencies that must send officers to certification programs or classes to learn cybercrime investigation techniques or for agencies that would need to hire a consultant or an additional officer who can perform such techniques.[201]

These costs are not, however, always proportionate to the level of punishment that a cyberharassment or cyberstalking statute

198. Hess, *supra* note 19.

199. *See id.*

200. *See Get a Quote*, CYBER INVESTIGATION SERVICES (2013), http://www.cyberinvestigationservices.com/internet-stalking/get-a-quote/.

201. As one study notes, some local law enforcement agencies may not just lack a computer expert; they may also lack an investigative officer who has relevant familiarity with the Internet in general. As a result, many law enforcement agencies may be unable to grasp the impact of cyberharassment and may even recommend that victims just turn off their computers. *See* U.S. DEP'T OF JUSTICE, CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY – A REPORT FROM THE ATTORNEY GENERAL TO THE VICE PRESIDENT 10 (1999), http://www.schmalleger.com/pubs/Cyberstalking_Report.pdf; *see also* Hess, *supra* note 19; CHRISTA MILLER, CYBER STALKING & BULLYING – WHAT LAW ENFORCEMENT NEEDS TO KNOW 2 (2006), http://www.ncdsv.org/images/CyberStalkingBullying—WhatLENeedstoKnow.pdf.

may carry. In the United States, sentences for cyberharassment can also vary widely in different states and at the federal level. Under the ICA, a perpetrator could face up to five years in prison and/or a fine of up to $1,000.[202] Under the CA, perpetrators can face up to two years in prison and/or a fine of up to $250,000.[203] In contrast, under California law, perpetrators may face no more than one year in prison.[204] In Michigan, unless the perpetrator violates a restraining order, a credible threat is issued against the victim and/or his family, the victim is a minor, or the defendant is repeat offender of the same cyberharassment crime, the perpetrator faces a jail sentence of two years and a fine of no more than $5,000.[205] In Massachusetts (where Quinn resided at the time of the blog posts and subsequent backlash), even if prosecutors were able to win a case against Gjoni, he would have faced no more than two and a half years in prison, with a possible fine of no more than $1,000.[206] In Arkansas and in New York, however, a conviction would only be considered a Class A misdemeanor.[207]

Because many of these laws were adapted from offline harassment laws, the sentences are comparable to offline harassment sentences.[208] Many of the sentences, however, are largely inadequate for online harassment. For example, investigating online harassment comes with costly challenges that may not be applicable to offline harassment investigations (e.g., if investigators do not have working knowledge of Internet investigation techniques).[209] If it would cost $2,500 and several months to determine the identity of a person sending a death threat to a victim,

202. 18 U.S.C.S. § 875(c) (2016).

203. 47 U.S.C.S. § 223 (2016); 18 U.S.C.S. § 3571 (2016).

204. CAL. PENAL CODE § 422 (Deering 2016).

205. MICH. COMP. LAWS SERV. § 750.411s (LexisNexis 2016).

206. MASS. ANN. LAWS ch. 265, § 43A(a) (LexisNexis 2016).

207. ARK. CODE ANN. § 5-41-108(b) (2016); N.Y. PENAL LAW § 240.30 (LexisNexis 2016).

208. For example, in California, a defendant may face up to a year in jail for cyberstalking; the same defendant, had his conduct occurred offline, would also face up to a year in jail or a fine of up to $1,000. *See* CAL. PENAL CODE §§ 422, 646.9. Notably, California's offline stalking law also includes provisions to further punish repeat offenders, while its cyberstalking law does not. *See* CAL. PENAL CODE §§ 653m(b), 646.9(c); *see also* ARK. CODE ANN. §§ 5-41-108(b), § 5-71-208(b) (both online and offline harassment is a Class A misdemeanor); MASS. ANN. LAWS ch. 265, § 43A(a) (LexisNexis 2016) (covers both offline stalking and cyberstalking); MICH. COMP. LAWS SERV. § 750.411s.

209. *See* U.S. DEP'T OF JUSTICE, *supra* note 201; *see also* Hess, *supra* note 19.

but a prosecutor could at best only obtain a sentence of two years and a $1,000 fine if the case were to be tried, it is easy to see why many prosecutors and law enforcement agencies may view the effort as disproportionate to the ultimate sentence that the accused would receive for the crime. Thus, the widely inconsistent definitions of what it means to harass or stalk a person over the Internet (that prevent many forms of cyberharassment from being covered within any particular jurisdiction), the widely inconsistent intent requirements or standards used in different jurisdictions, the lack of law enforcement training on online crimes, and the disproportionality between the cost of providing such training and the sentences imposed for cyberharassment and cyberstalking crimes in many jurisdictions each contribute to a U.S. body of law that leaves victims of cyberharassment and cyberstalking vulnerable.

B. Problems and Solutions Found in International Cyberharassment and Cyberstalking Laws

International approaches to cyberharassment and cyberstalking law also have their own issues that can prevent them from adequately criminalizing cyberharassment and cyberstalking. As is the case with the United States, international, Canadian, and Australian law have different definitions of cyberharassment and cyberstalking that, to varying degrees, do not allow for a full variety of cyberharassment and cyberstalking acts to be criminalized. In their attempts to cover more versions of cyberharassment and cyberstalking, at least some Canadian laws have clashed with Canadian constitutional laws. On the other hand, there are features of these laws that do solve some issues that remain in U.S. law. For example, the Canadian Criminal Code includes an intent standard that clarifies what prosecutors need to prove to satisfy elements of cyberharassment and cyberstalking. Additionally, Australian cyberharassment and cyberstalking laws include numerous mechanisms that broaden the scope of the written law and which provide a staggered sentencing structure that includes stricter punishments for these types of crimes. Each of these features are useful for determining ways to improve (or not change) existing cyberharassment and cyberstalking laws in other jurisdictions.

1. Canada

While Canadian federal law is a slight improvement over U.S. law due to its inclusion of an intent standard, nonetheless, it is not perfect. As previously noted, the Canadian Criminal Code requires the accused to act "knowing that another person is harassed or recklessly as to whether the other person is harassed."[210] Canada's Criminal Code, which explicitly describes both specific and reckless standards of intent for the accused, also requires that the victim reasonably fear for his or her safety in order for the accused to be convicted.[211] Thus, victims such as Zoe Quinn, who are undoubtedly harmed by having personal and private information disclosed to the public online, but who may not fear for their personal safety as a result of those specific actions, may be unable to seek legal recourse in Canada.[212] Canadian lower courts have varied interpretations of the fear element of the statute,[213] with the most liberal courts being willing to waive the element as a requirement in extreme cases, including those involving the disclosure of intimate or obscene content.[214] There remains a question, however, of how this element would be interpreted by the Canadian Supreme Court.[215] This results in inconsistency in how the Canadian Criminal Code is then applied.[216]

Similarly, Canadian provinces also lack effective cyberharassment legislation. Just recently, the Nova Scotia Supreme Court ruled that the CSA violates Subsections 2(b) and 7 of the Canadian Charter of Rights and Freedoms, which protect free speech and "principles of fundamental justice,"[217] and invalidated the

---

210. R.S.C. 1985, c C-46, s 264(1) (Can.).

211. *Id.*; *see also* Levin, *supra* note 133.

212. Levin, *supra* note 133.

213. *Id.*

214. *See* R. v. Barnes, 2010 ABQB 285 (Can.).

215. Levin, *supra* note 133. As in the U.S. federal courts system, the Canadian Supreme Court is the highest appellate court for cases in the federal system and renders final judgments regarding how to interpret statutory and common law matters. *See The Judicial Structure*, CAN. DEP'T JUST. (July 25, 2015), http://www.justice.gc.ca/eng/csj-sjc/just/07.html.

216. *See* Crouch v. Snell, 2015 NSSC 340, para. 141; Ruskin, *supra* note 136.

217. Subsection 2(b) guarantees "freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication." Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, *being* Schedule B to the Constitution Act, 1982, c 11, s 2(b) (Can.). Section 7 guarantees "the right to life, liberty and security of the person and the right

entire act.[218] Specifically, in the seminal case, *Crouch v. Snell*, the court ruled that speech that "falls short of violence or threats of violence . . . [are] within the sphere of conduct protected by s.2(b)"; thus, the CSA's prohibition of speech that was nonthreatening in nature (such as speech that was merely humiliating) violated Subsections 2(b) of the Canadian Charter of Rights and Freedoms.[219] Further, the court ruled that the CSA's attempt to control or restrict speech (i.e., by restricting harassing or humiliating speech) violated fundamental freedoms embodied in the Canadian Charter of Rights and Freedoms.[220] As of the date of this publication, the Nova Scotia Legislature has not yet passed legislation to replace the CSA. Thus, Nova Scotia, the pioneer in Canadian online harassment law, has been forced to return to the drawing board to construct more limited legislation. Being that the CSA was deemed unconstitutional in Canada, it is also unlikely to be passed in the United States, where legislatures and courts tend to be more hesitant about restricting free speech.[221] For example, in the United States, only narrow categories of speech are constitutionally unprotected (including true threats, speech intended to incite others to commit criminal conduct, and some expression of highly confidential information).[222] A law such as the CSA, which restricts the transmission of not only threats but also content that may humiliate a person, would ultimately not fall under these narrow categories of speech. Thus, were the U.S. Congress to pass a similar law, it would just as quickly be in the same position as the legislature of Nova Scotia.

Ontario's cyberharassment tort carries with it additional issues. For example, Ontario's civil tort, as it is defined currently, only covers the dissemination of embarrassing private facts.[223]

---

not to be deprived thereof except in accordance with the principles of fundamental justice." *Id.* s 7. The "principles of fundamental justice" have generally referred to "'basic tenets and principles'" of the Canadian judicial process, such as procedural fairness and a general judicial duty to act fairly in legal proceedings. *See* J. M. Evans, *The Principles of Fundamental Justice: The Constitution and the Common Law*, 29 OSGOODE HALL L.J. 51, 55 (1991).

218. *See Crouch*, 2015 NSSC, para. 221.

219. *Id.* para. 106.

220. *Id.* paras. 111–12.

221. *See* Kent Greenawalt, *Free Speech in the United States and Canada*, 55 LAW & CONTEMPORARY PROBLEMS, no. 1, 1992, at 5, 8.

222. *See* Volokh, *supra* note 8.

223. *Cyberbullying and the Law, supra* note 141.

The tort, therefore, does not cover many forms of cyberharassment or cyberstalking, including threats or other forms of harassment that do not involve divulging embarrassing private information. Further, as the law is a tort, a perpetrator must have a duty to the victim to not disseminate the private information (or, generally speaking, must violate a duty to the victim to be found liable for the offense).[224] Many cyberharassment or cyberstalking perpetrators, however, are unlikely to have an obligation or a duty to the victim to not release information. For example, there would generally be no understanding between a victim and an anonymous perpetrator that the latter would not release the victim's private information. Since the tort was first created in 2016, it is unclear, as of the time of this publication, how far courts would be willing to stretch a duty between a victim of cyberharassment and a party who acts against the victim, and the extent to which the tort will be applicable to instances where parties do not know each other or have established an understanding of confidence.

On a positive note, cyberharassment crimes in Canada consistently allow for strong punishments against defendants convicted of cyberharassment. For example, cyberharassment convictions can carry a prison term of up to ten years in Canada under federal law.[225] Even under Nova Scotia's now-defunct law, cyberbullying was a tort subject to general, special, aggravated, and punitive damages.[226] The higher jail sentences in Canada, if similarly implemented in the United States, may provide the proper incentive for U.S. law enforcement to investigate more cyberharassment cases.[227] Said another way, as law enforcement has specifically pointed to the small maximum sentences for various cyberharassment and cyberstalking crimes in the United States as a hurdle for justifying investigating such crimes,[228] the United States should take note of the fact that countries, such as Canada, have passed statutes that carry much harsher sentences and consider raising the sentences of its own cybercrimes to more closely reflect those of other nations.

224. *See* Jane Doe 464533 v. N.D., 2016 ONSC, para. 21.
225. *See* R.S.C. 1985, c C-46, s 264(1) (Can.).
226. Cyber-safety Act, S.N.S. 2013, c 2, s 3(1)(b) (Can.).
227. *See* Hess, *supra* note 19.
228. *Id.*

2. Australia

Similar to U.S. statutes, under portions of the ACCA, proving the intent of the perpetrator can be difficult due to the nature of the intent required for certain portions of the statute.[229] Portions of the ACCA require different showings of intent by the accused, including (1) intent to commit a serious offence, (2) intent to cause a victim to fear that a threat would be carried out, or (3) intent to cause a victim to believe a dangerous substance or object was placed in a particular location.[230] For situations such as Zoe Quinn's, where many of the perpetrators are anonymous and may have only sent one message to Quinn, it may still be easy for defendants to simply deny that they had an intent to harass or harm the victim.[231] Because the victim's experience is not taken into account, a court need not consider negligence or recklessness on the part of the perpetrator.[232]

Taken in the aggregate, however, the ACCA appears to provide adequate protections for all types of cyberharassment. Namely, the ACCA covers a number of different forms of cyberharassment and cyberstalking, including threats, defamation, disclosing private information, and other types of cyberharassment and cyberstalking.[233] The ACCA also requires multiple degrees of intent for particular types of cyberharassment and cyberstalking (including specific intent for the accused for the crimes that carry higher sentences and general intent for the accused for crimes that carry lesser sentences).[234] Finally, the ACCA includes provisions that guarantee prosecution of persons with some kind of connection to Australia if the conduct violates at least some foreign laws.[235]

Importantly, the ACCA does not necessarily require that a threat be sent directly to the victim, allowing, for example, for charges to be brought against perpetrators who post threats on

229. *See* Fukuchi, *supra* note 25.

230. *See Criminal Code Act 1995* (Cth) ch 10 div 474 sub-div C s 474.14–474.17 (Austl.).

231. *Id.*

232. Australian courts take the effects of the alleged cyberharassment or cyberstalking on the victim into consideration with respect to sentencing, but they do not factor into the determination whether or not the defendant is actually guilty. *See Cullen v White* [2003] WASC 153 (Austl.); *R v Hampson* [2011] QCA 132 (Austl.).

233. *See supra* Part II.

234. *Id.*

235. *Id.*

their personal Facebook page that are directed toward other persons.[236] Additionally, similar to the Canadian Criminal Code law, the ACCA tends to be more punitive of defendants convicted of cyberharassment than U.S. federal or state law. ACCA § 474 includes staggered sentencing depending on the severity of the crime. For example, for death threats, perpetrators can receive up to ten years in jail.[237] For threats of harm, perpetrators can receive up to seven years in jail.[238] And for conduct that is menacing or offensive, a perpetrator could face up to three years in jail.[239] As with Canadian sentences, Australia's higher jail sentences could certainly justify the extra months that may be spent investigating online crimes and could attach more importance to cyberharassment claims, which could help convince law enforcement to invest the extra resources necessary to investigate such crimes.[240]

Further, including general intent standards on the part of the accused, for at least some crimes, allows for easier prosecution of those forms of cyberharassment and cyberstalking. For example, by not requiring a finding of specific intent on the part of the accused, prosecutors can pursue cases against defendants, even when their intentions may be ambiguous or difficult to prove. On the other hand, by still including a specific intent standard for the forms of cyberharassment and cyberstalking that carry

---

236. In a recent landmark case, an Australian man pled guilty to such a charge after posting rape threats on his Facebook page. *See* Elahe Izadi, *Rape Threats on a Stranger's Facebook Photo Could Land a Man in Prison. Why That's a Big Deal*, WASH. POST (June 22, 2016), https://www.washingtonpost.com/news/the-intersect/wp/2016/06/22/rape-threats-on-a-strangers-facebook-photo-could-land-a-man-in-prison-why-thats-a-big-deal/?tid=sm_fb. The defendant did not ultimately serve jail time, as the magistrate judge ultimately decided that the comments did not incite rape and that the defendant had paid for his offensive comments already by being maligned at trial. *See Zane Alchin Given Good Behavior Bond for Making Facebook Threats About Olivia Melville Tinder Profile*, ABC NEWS (July 28, 2016, 10:35 PM), http://www.abc.net.au/news/2016-07-29/internet-troll-zane-alchin-sentenced-over-tinder-profile-threat/7671674. The notion that a person could be convicted of such a crime at all, however, demonstrates an interesting difference in how Australian law is currently equipped to deal with online harassment in comparison to U.S. law (in view of *Elonis*).

237. *See Criminal Code Act 1995* (Cth) ch 10 div 474 sub-div C s 474.15(1) (Austl.).

238. *Id.* s 474.15(2).

239. *Id.* s 474.17(1).

240. *See* Hess, *supra* note 19.

higher prison sentences, the ACCA still requires proof that the accused intended to perform actions that are proportional to the higher prison sentence. In doing so, the ACCA prevents defendants from facing extended prison sentences without a determination that the defendant intended to commit a serious offense.

Finally, Australia's provisions concerning foreign law address the globalized nature of online communications. For example, prosecutors in Australia can rely on provisions that criminalize Australians' cyberharassment or cyberstalking conduct that occurs both outside Australia, or occurs inside Australia but incites others outside of Australia to commit such actions. In this sense, even when some of the conduct is not fully performed within Australian borders or between Australian citizens, online harassment and stalking can still be addressed. By criminalizing activity that extends past Australia's borders via the Internet, and which violates laws of other nations, the ACCA addresses crimes that, inherently, allow Australian citizens to harass or stalk other Australian citizens, or citizens in other countries, while also taking into account the severity of foreign nations' criminal statutes in the process.

IV. A PROPOSED MODEL STATUTE FOR DEALING WITH CYBERHARASSMENT AND CYBERSTALKING CRIMES

To address the problems with existing U.S. cyberharassment law, the United States must adopt a new law that clarifies existing legal doctrines and incentivizes law enforcement to investigate cyberharassment crimes. Specifically, the proposed Model Statute offered herein seeks to create a uniform definition of cyberharassment with an explicit intent standard that U.S. courts can utilize in future litigation. Further, the proposed Model Statute seeks to include sentencing structures that can encourage law enforcement to investigate cyberharassment crimes. This Part will then apply the proposed Model Statute to the facts of both Zoe Quinn and the victim in *Elonis* to illustrate how the amendments would substantially help prosecute these and similar cyberharassment cases.

A. Analyzing the Components of the Proposed Model Statute

The proposed Model Statute would amend the existing ICA to address many of the problems facing current cyberharassment and cyberstalking laws in the United States. As an amendment to a federal law, the proposed Model Statute would ensure that

the types of cyberharassment and cyberstalking crimes covered under the statute would affect all U.S. citizens uniformly, regardless of the states where the defendant or the alleged victim reside. To define a clearer standard of intent for the ICA, the proposed Model Statute would include a recklessness standard, similar to that found in the Canadian Criminal Code.[241] Under the proposed Model Statute, anyone who "knowingly or recklessly" transmits threatening or harassing communications will be found in violation of the statute.[242] This amendment will solve the primary point of contention in *Elonis*[243] by specifying the standard of intent required for each element of the statute. Specifically, the proposed Model Statute will allow courts to know the particular intent standard required for a defendant to have violated the statute and will also provide the court (and juries) some flexibility in how they analyze the defendant's perspective.[244] The proposed Model Statute would further incorporate aspects of existing criminal laws that would broaden the scope of existing U.S. federal law, such as criminalizing activity that encourages repeat behavior with third parties and criminalizing activity other than true threats.

The proposed Model Statute would also include a lesser offense with a general intent standard, such that a defendant need not intend to cause distress to the victim, so long as the defendant did in fact act in a way that caused such distress or encouraged others to cause distress to the victim.[245] This element both reflects how some U.S. state jurisdictions[246] and Australia[247] handle intent standards for cyberharassment and makes explicit what a defendant needs to know (or does not need to know) to

241. *See* R.S.C. 1985, c C-46, s 264(1) (Can.).

242. *See infra* app., sec. 3(a).

243. Elonis v. United States, 135 S. Ct. 2001, 2013 (Alito, J., concurring in part and dissenting in part). The use of a "recklessness" standard would not only clarify the lens through which to analyze the defendant's actions but would also specify a standard that Justices Alito and Thomas have already sanctioned in *Elonis*. *See id.*

244. This standard has been adopted by states as well, including California. *See* CAL. PENAL CODE § 653m (Deering 2016).

245. *See infra* app., sec. 3(c)(e).

246. *See* Fukuchi, *supra* note 25, app. at 331–38.

247. *Criminal Code Act 1995* (Cth) ch 10 div 474 sub-div C s 474.17(1) (Austl.).

have violated the statute.[248] This would also serve as a solution to a major point of contention in *Elonis*, where intent standards under the ICA were (and to an extent, still are) ambiguous.[249]

The proposed Model Statute would also broaden the geographical scope of existing U.S. law. For example, the proposed Model Statute would include provisions specifying that a person who violates "a cybercrime law of a foreign nation" may still be liable under the proposed Model Statute.[250] Similar to how such provisions work in Australia, such an amendment would be able to provide further protections for persons who are attacked across national borders.[251]

Finally, the proposed Model Statute would provide multiple incentives for law enforcement to investigate cyberharassment crimes. For example, the proposed Model Statute would revise the ICA to include the staggered approach to punishment found in Michigan law[252] and in Australian law.[253] Under the staggered approach, previous convictions under the proposed Model Statute would result in larger fines (e.g., $2,500–$5,000 in additional fines) and/or prison sentences (e.g., up to six years of additional prison time).[254] Further, the proposed Model Statute would include a provision that would charge a defendant an additional fine to be applied toward the costs associated with the investigation of the defendant's actions.[255] Specifically, a percentage of the costs associated with the investigation would be paid by the defendant, should the defendant be found guilty of the crime. Because law enforcement has noted that costs associated with investigating such crimes can be prohibitive,[256] specifying that the fines be directly applied to funding law enforcement costs for

248. In his dissenting opinion, U.S. Supreme Court Justice, Clarence Thomas, expressed that general intent was already inherent in the original statute. *See Elonis*, 135 S. Ct. at 2018 (Thomas, J., dissenting). The proposed amendments would therefore make explicit what could already be reasonably considered an inherent characteristic of the existing statute.

249. *See id.*

250. *See infra* app., sec. 3(c)(f).

251. *See* Urbas, *supra* note 157, at 7.

252. MICH. COMP. LAWS SERV. § 750.411s (LexisNexis 2016).

253. *Criminal Code Act 1995* (Cth) ch 10 div 474 sub-div C ss 474.15(1)–(2), 474.17(1).

254. *See infra* app., sec. 3(c)(g).

255. *See id.* sec. 3(c)(i).

256. Hess, *supra* note 19.

investigating the facts of the case would help to empower law enforcement to investigate such crimes.

B. Applying the Proposed Model Statute to Zoe Quinn's Experience

To an extent, Quinn's multifaceted experiences with harassment would have been better served under the proposed Model Statute.[257] The proposed Model Statute's inclusion of instances where a victim feels threatened or harassed, regardless of whether a perpetrator's threat is credible or intended to harass,[258] would have provided prosecutors with a cause of action against the anonymous harassers that sent her death threats and other distressing messages.[259] The proposed Model Statute would also have given prosecutors a cause of action against Gjoni, whose blog posts could arguably be seen as harassment by a reasonable person, even if Gjoni did not intend for Quinn to feel harassed or threatened.[260] The proposed Model Statute would require inquiry into whether a reasonable person would feel frightened, threatened, or harassed. This would protect persons who make comments that are merely annoying or hurtful and persons who send messages that a reasonable person would interpret humorously. Additionally, the proposed Model Statute would provide a way to prosecute individuals who encourage or incite others to commit additional harassment against the victim,[261] which, in Quinn's circumstances, would have potentially given prosecutors another claim against Gjoni, due to the fact that his blog posts likely incited others to send death threats to

257. There are many aspects of cyberharassment and cyberstalking that are not intended to be addressed by the ICA and would not be addressed by the proposed Model Statute. Such offenses would include defamation and revenge porn. Addressing solutions to the myriad types of cybercrime committed against Quinn would be beyond the scope of this Note. Instead, this Note primarily seeks to prevent threatening communications over the Internet, including those that inspire others to participate in subsequent harassment.

258. *See infra* app., sec. 3(c)(e).

259. It can be difficult to argue that a threat is credible when it is sent by an anonymous harasser. *See* Baer, *supra* note 75, at 160–61; Goodno, *supra* note 77, at 135–36. Creating causes of action that do not require the threat to be credible, therefore, helps persons such as Quinn, who cannot prove that their anonymous harassers could truly pose imminent threats to their safety.

260. *See infra* app., sec. 3(c)(e).

261. *See id.* sec. 3(c)(e). A similar element exists in Michigan law. *See* MICH. COMP. LAWS SERV. § 750.411s (LexisNexis 2016).

Quinn.[262] Specifically, a prosecutor would have been able to use the proposed Model Statute to charge Gjoni with the crime of acting in a harassing manner, by encouraging other parties to harass Quinn through hacking attempts and anonymous messages, among others. This portion of the proposed Model Statute would have applied irrespective of whether Gjoni intended to harass or intended to incite additional harassment against Quinn. In other words, the proposed Model Statute would have provided several avenues of justice for Quinn who, under Massachusetts state law, laws of states other than Massachusetts, and existing federal law, would otherwise largely be unable to hold Gjoni and anonymous Internet harassers legally accountable for their vicious actions.[263]

C. Applying the Proposed Model Statute to Elonis

When applied to *Elonis*, the proposed Model Statute would have allowed the government to prevail against the defendant. The principal point of contention in the *Elonis* decision concerned which standard of intent to apply to the defendant's *mens rea*: in other words, whether the standard of intent could be general intent[264] or whether the standard had to be more than general intent.[265] The proposed Model Statute removes this uncertainty by specifying that "recklessly" transmitting threatening language would violate the statute.[266] Further, the proposed Model Statute would also include a lower-level offense that would only require general intent on the part of the defendant (i.e., that would not require the defendant to intend for the communication to cause another to feel threatened or otherwise distressed).[267] With either the reckless standard or the general intent standard, the point of contention in *Elonis* would be rendered moot. The court would have a clear intent standard with which to instruct the jury, depending on which section of the proposed Model Statute was being used to prosecute the defendant.

For example, the proposed Model Statute would have explicitly advised the court that, for the highest-level offense (having a

262. *See generally* Elise, *supra* note 3; Dewey, *supra* note 2.
263. Volokh, *supra* note 8.
264. *See* Elonis v. United States, 135 S. Ct. 2001, 2018 (2015) (Thomas, J., dissenting).
265. *See id.*
266. *See infra* app., sec. 3(a).
267. *See id.* sec. 3(c).

sentence of up to ten years and a fine of $1,000–$2,500), the jury would need to determine whether the defendant knowingly or recklessly created his threatening posts. Alternatively, for the lower-level offense (having a sentence of a year and a fine of $1,000–$2,500), the jury would have been instructed to determine whether the defendant's posts would have caused a reasonable person to feel terrorized, frightened, or otherwise distressed, regardless of whether the defendant knew or intended the communication to have this effect on the recipient. Thus, even if the government had been unable to prove that the defendant knew that his posts would be interpreted as a threat, the defendant would still have been found guilty under the proposed Model Statute, so long as the defendant was found to be acting recklessly or so long as the defendant was being charged with the lesser offense. Additionally, because the intent standard of both offenses is explicitly outlined, future litigants would not run the risk of losing cases due to an ambiguity over the standard required to convict a defendant.

CONCLUSION

Individuals all over the globe continue to face various forms of cyberharassment.[268] As it stands today in the United States, a person targeted for cyberharassment has limited recourse against his or her harassers.[269] Whether due to inconsistent or vague definitions of cyberharassment[270] or law enforcement that is too ill-equipped, unwilling, or unable to fully investigate cyberharassment cases, restitution and legal recourse in the United States is inadequate.[271] By amending existing U.S. federal law to address these issues, the amendments to the Model Statute proposed herein would resolve numerous uncertainties. The proposed Model Statute would provide much-needed updates to the federal definitions of cyberharassment and cyberstalking, allowing cyberharassment and cyberstalking to be regulated in a uniform way across the country. The proposed Model Statute would also simultaneously provide causes of action for victims, such as those in *Elonis* and Zoe Quinn, that would incentivize law enforcement to investigate cyberharassment and

268. *See* Dewey, *supra* note 2; Dewey, *supra* note 12; Watt, *supra* note 12; Tsukayama, *supra* note 12.

269. *See supra* Part III.

270. *See supra* Parts II, III.

271. *See supra* Part III.

cyberstalking incidents to uncover evidence needed to successfully prosecute such crimes. Better yet, modifying U.S. law to share features also found in the cyberharassment laws of other nations, such as Canada and Australia, would further embrace the international nature of the Internet (namely, that harassers may perpetrate cyberharassment from anywhere in the world).[272] With the proposed Model Statute, Zoe Quinn could have prevented her ex-boyfriend from publishing private information to fuel an Internet war against her, the government could have prevented individuals from posting violent threats against their spouses over the internet, and countless others could have used the overarching federal law to obtain consistent legal recourse when faced with online harassment. If the United States truly wishes to save other citizens from the traumas and life-altering effects of cyberharassment and cyberstalking, it must change its laws to address more victims and to entice law enforcement to investigate the crimes to ensure that justice is obtained for these victims.

A. Meena Seralathan[*]

272. Because the Internet is accessible across the globe (*see Internet Usage Statistics*, *supra* note 74), it could one day be imperative to establish international standards for cyberharassment, to allow for criminal prosecution of perpetrators who act across national borders. Such a proposal, however, is beyond the scope of this Note.

* B.S., Haverford College (2011); J.D. Candidate, Brooklyn Law School (2017); Executive Articles Editor, *Brooklyn Journal of International Law* (2016–2017). I would like to thank the *Journal* staff for helping to improve the quality of this Note; my family (particularly my parents, who sacrificed to give me a chance to obtain my undergraduate degree); my fiancé, for helping me get through three years of law school; and the millions of victims of cyberharassment and cyberstalking across the globe, whose unwavering bravery in the face of online extremism inspired me to write about their experiences.

APPENDIX

A MODEL STATUTE

To amend Title 18 United States Code, with respect to cyberharassment.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE

This Act may be cited as the "Model Cyberharassment Prevention Act."

SECTION 2. FINDINGS

Congress finds the following:

[*supra* Part I]

SECTION 3. CYBERHARASSMENT

(1) IN GENERAL. – Section 875 of title 18, United States Code, is amended by replacing Subsection 875(a) with the following:

> (a) Whoever *knowingly or recklessly* transmits in interstate or foreign commerce any communication containing any demand or request for a ransom or reward for the release of any kidnapped person, shall be fined under this title or imprisoned not more than twenty years, or both.

(2) Section 875 of title 18, United States Code, is amended by replacing Subsection 875(c) the following:

> (c) Whoever *knowingly or recklessly* transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than ~~five~~ ten years, or both.

(3) Section 875 of title 18, United States Code, is amended by adding after Subsection 875(d) the following:

> (e) Whoever transmits in interstate or foreign commerce any communication that would cause a reasonable person who is a subject of the communication to suffer substantial emotional distress, and would cause a reasonable person who is a subject of the communication to feel terrorized, frightened, intimidated, threatened, harassed, or molested, whether due to the nature of the communication or the foreseeable effect of the communications on others, shall be fined under this title or imprisoned not more than one year, or both.
>
> > (i) A person who transmits such a communication need not know or intend that the communication would cause a subject of the communication to suffer substantial emotional distress or to feel terrorized, frightened, intimidated, threatened, harassed, or molested.
>
> (f) Whoever knowingly or recklessly transmits in interstate or foreign commerce any communication that would be prohibited under United States law, or a cybercrime law of a foreign nation had the crime been committed in the United States, shall be fined under this title or imprisoned not more than three years, or both.
>
> (g) Whoever commits any of Subsections 875(a)–(f), who has been previously convicted of any of Subsections 875(a)–(f), shall be liable for an additional fine of no less than $2,500, and no more than $5,000, or imprisoned for an additional term of no more than six years, or both.
>
> (h) For purposes of Subsections 875(a)–875(c), and 875(e)–(f), the fine shall be no less than $1,000, and no more than $2,500.
>
> (i) Whoever commits any of Subsections 875(a)–(f), shall be fined, in addition to the fine specified in Subsection 875(g) or 875(h), an amount equaling a percentage of

costs associated with the investigation of said communications described in Subsections 875(a)–(f), said percentage being no less than 25 percent, and the total value of the fine not to exceed $10,000.