ONLINE HARASSMENT: A LEGISLATIVE SOLUTION

EMMA MARSHAK*

TABLE OF CONTENTS

I. INTRODUCTION

A journalist publishes an article; rape threats follow in the comments.[1] An art curator has a conversation with a visitor to her gallery; he sends her

* B.A., Cornell University, 2010; J.D., Harvard Law School, 2016. The author would like to thank Professor Alex Whiting for his guidance and the Cyber Crime Division of the Massachusetts Attorney General's Office for the experience and insight.

[1] *See* Lindy West, *If Comedy Has No Lady Problem, Why Am I Getting So Many Rape Threats?*, JEZEBEL (June 4, 2013), http://jezebel.com/if-comedy-has-no-lady-problem-why-am-i-getting-so-many-511214385 [https://perma.cc/J2AW-4YFP]. Many people issued threats to the author in response to one of her articles. One person, who goes by the name "Mylocalman," stated that he "want[s] to rape [the author] with a traffic cone." *Id.; see also* Amanda Hess, *Why Women Aren't Welcome on the Internet*, PACIFIC STANDARD (Jan. 6, 2014), http://www.psmag.com/navigation/health-and-behavior/women-arent-welcome-internet-72170/ [https://perma.cc/KD6S-RBL2]. Threats issued by a user named "headlessfemalepig" included "Happy to say we live in the same state. Im [sic] looking you up, and when I find you, im [sic] going to rape you and remove your head" and "You are going to die and I am the one who is going to kill you. I promise you this." *Id.*

letters from jail (where he was imprisoned for stalking Ivanka Trump[2]) and, upon his release, escalates his death threats from her to her employers.[3] A video game developer releases a game, and she is promptly inundated with "shocking, gruesome, specific, and obscene [threats], involving many variations on murder and rape."[4] A reporter asks a politician a pointed question, and the politician's supporters harass her online and show up at her apartment; she hires a security detail.[5]

What do all of these real incidents have in common? The threat was issued over the internet, and the prosecution was unsuccessful. Online threats and harassment are a growing problem as life moves online, and the current set of state laws, which were mostly developed in the 1990s, generally lack the vocabulary and framework to address criminal behavior that occurs in cyberspace rather than physical space. Furthermore, while all laws governing speech must respect the First Amendment, the "true threat" doctrine, an exception permitting prosecution, has been applied inconsistsently in the wake of *Elonis v. United States*.[6]

In the four examples given above, the perpetrators were strangers to the victims. This is common in cases of online harassment and creates unique enforcement challenges. Therefore, this Note uses a classification system that differentiates "familiar perpetrators" from "unfamiliar perpetrators." Familiar perpetrators are identifiable, usually because they issued the threats under their own name. Often some sort of relationship exists between the

---

[2] *See* Melissa Grace, *Ivanka Trump's Stalker Pleads Guilty to Aggravated Harassment Charge—and Is Set Free*, DAILY NEWS (Feb. 9, 2012, 1:16 PM), http://www.nydailynews.com/new-york/ivanka-trump-stalker-pleads-guilty-amp-released-article-1.1019847 [https://perma.cc/E2GJ-DD2J].

[3] *See* Telephone Interview with Lenora Claire (Feb. 3, 2016) [hereinafter 2016 Claire Interview]; *see also* Joanna Rothkopf, *What Do You Do When a Notorious Celebrity Stalker Starts Stalking You?*, JEZEBEL (Dec. 10, 2015, 4:10 PM), http://jezebel.com/what-do-you-do-when-a-notorious-celebrity-stalker-start-1737619684 [https://perma.cc/UK53-PJAU]; *Art Curator Stalked by Schizophrenic Man Pushes for Change in Law*, CRIME WATCH DAILY (Jan. 14, 2016), http://crimewatchdaily.com/2016/01/11/la-art-curator-targeted-by-schizophrenic-stalker/ [https://perma.cc/GC56-JLMN].

[4] David Whitford, *Brianna Wu vs. the Gamergate Troll Army*, INC. (April 2015), http://www.inc.com/magazine/201504/david-whitford/gamergate-why-would-anyone-want-to-kill-brianna-wu.html [https://perma.cc/T84K-N2VV].

[5] *See* Jim Rutenberg, *Megyn Kelly's Cautionary Tale of Crossing Donald Trump*, N.Y. TIMES (Nov. 15, 2016), https://www.nytimes.com/2016/11/16/business/media/megyn-kellys-cautionary-tale-of-crossing-donald-j-trump.html [https://perma.cc/HMR2-6VDW]; *see also* Marin Cogan, *In 2016, the Trolls Finally Escaped the Internet*, ESQUIRE (Dec. 21, 2016), http://www.esquire.com/news-politics/a51713/how-internet-trolls-won-in-2016/ [https://perma.cc/G7FW-K449] (telling the story of Jennifer Jones, whose four-year-old daughter's photo was turned into an anti-Clinton meme). One example of an online threat that was prosecuted is "Pizzagate," where a community full of online threats inspired a man to shoot a rifle in a restaurant. He was arrested. *See generally* German Lopez, *Pizzagate, the Fake News Conspiracy Theory that Led a Gunman to DC's Comet Ping Pong, Explained*, VOX (Dec. 8, 2016, 11:15 AM), http://www.vox.com/policy-and-politics/2016/12/5/13842258/pizzagate-comet-ping-pong-fake-news [https://perma.cc/9HHD-NWCV].

[6] *See* 135 S. Ct. 2001, 2012–13 (2015). The Supreme Court declined to set a clear national standard for mens rea.

perpetrator and the victim: an ex-spouse, a coworker, a neighbor, a former student, etc. Frequently, familiar perpetrators live in the same geographic area (and therefore generally the same jurisdiction) as the victim. For these reasons, traditional law enforcement tools, including protective orders, can be effective, and the existence of binding legal precedent simplifies prosecutions. While victims who are harassed and threatened by familiar perpetrators face the same difficulties as other victims in getting police to take their threats seriously, a prosecution can follow relatively easily once an investigation has begun.

Unfamiliar perpetrators are exemplified by the anonymous internet troll.[7] The threats are signed not with legal names, but rather usernames like "Death to Brianna"[8] or "headlessfemalepig."[9] Half of the victims of online harassment do not know the perpetrators.[10] A successful prosecution requires the investment of law enforcement time and resources, such as subpoenas, to track the usernames and accounts down from IP address to internet provider to physical address. Once the perpetrator has been located (assuming no precautionary measures were taken, such as routing communications through a server inaccessible to American law enforcement), the perpetrator will often be in a different state and jurisdiction from the victim. Successful prosecutions are therefore extremely rare.

This Note lays out the reasons why online harassment is a problem, including its scope and measurable economic impact. After discussing current state laws, and why the patchwork of laws regulating online threats and harassment especially inhibits prosecution of unfamiliar perpetrators, this Note articulates problems with the status quo of law enforcement and investigation of online harassment. This Note then suggests a three-part solution. First, a common model statute, such as the one proposed in Part V.a. and the Appendix, *infra*. Today, the same crime may be defined differently in different states or may not even be illegal at all under antiquated statutes that fail to address electronic communications. A common statute will standardize

---

[7] For definitions and explanations of the noun "troll" and the verb "trolling," see generally Elise Moreau, *Internet Trolling: How Do You Spot a Real Troll?: How Internet Trolling Affects Us All Online*, LIFEWIRE, http://webtrends.about.com/od/Internet-Culture/a/What-Is-Internet-Trolling.htm [https://perma.cc/N6LE-6C82] (last updated Dec. 16, 2016); Zoe Williams, *What is an Internet Troll?*, GUARDIAN (June 12, 2012), http://www.theguardian.com/technology/2012/jun/12/what-is-an-internet-troll [https://perma.cc/7HYM-BEVX]. *See also* Patricia Hernandez, *10 Former Internet Trolls Explain Why They Quit Being Jerks*, KOTAKU (Aug. 7, 2015, 4:00 PM), http://kotaku.com/10-former-internet-trolls-explain-why-they-quit-being-j-1722649439 [https://perma.cc/36B4-7GBR]; Amanda Hess, *How the Trolls Stole Washington*, N.Y. TIMES: MAGAZINE (Feb. 28, 2017), https://www.nytimes.com/2017/02/28/magazine/how-the-trolls-stole-washington.html?emc=eta1&_r=0 [https://perma.cc/L9D6-E7Z5].

[8] Lisa Eadicicco, *This Female Game Developer Was Harassed So Severely on Twitter She Had to Leave Her Home*, BUS. INSIDER (Oct. 12, 2014, 11:46 AM), http://www.businessinsider.com/brianna-wu-harassed-twitter-2014-10 [https://perma.cc/4FCS-JJYS].

[9] Hess, *supra* note 1.

[10] PEW RESEARCH CTR., ONLINE HARASSMENT 5 (Oct. 22, 2014), http://www.pewinternet.org/files/2014/10/PI_OnlineHarassment_72815.pdf [https://perma.cc/6K7W-2VLF].

the approach to online threats and harassment across jurisdictions, increase efficiency through the use of uniform training materials, and improve cooperation and coordination between multiple law enforcement agencies. Second, a national evidence laboratory, discussed in Part V.b., *infra*, would solve the problem of disparate state resources devoted to digital forensic evidence. Third, updated and readily available training materials and procedures like those proposed in Part V.c., *infra*, will educate the police officers who receive initial reports of harassment on how best to respond and on what resources they can direct the victim to access.

II. Why is Online Harassment a Problem?

a. The Scope of the Problem

Anyone who read the comments on news articles about the 2016 election or who regularly reads message boards sees commenters attacking authors and each other, so it should come as no surprise that 72% of internet users in 2016 reported witnessing online harassment.[11] In fact, vitriol in comment sections is such a common problem that news organizations without the resources to moderate comments sections sometimes turn them off completely.[12] What may be more surprising is the violence pervading that harassment—and its disproportionate impact on women. Most women under thirty years old have been harassed online; it is three times more likely that online harassment will escalate to attempted physical harm to young women than to older adults.[13] More broadly, of the internet users who reported witnessing online harassment in 2014, 25% had seen physical threats, 19% had witnessed sexual harassment, and 18% had witnessed stalking.[14] Certain age groups are targeted more than others, but "young women, those [aged eighteen to twenty-four], experience certain severe types of harassment at disproportionately high levels: 26% of these young women have been stalked online," as opposed to only 7% of men aged eighteen to twenty-four and 8% of all internet users, "and 25% [of young women] were the target of online

[11] Amanda Lenhart et al., Online Harassment, Digital Abuse, and Cyberstalking in America, Data & Society 12 (Nov. 21, 2016), https://datasociety.net/pubs/oh/Online_Harassment_2016.pdf [https://perma.cc/DE5Z-GFPP] [hereinafter Data & Society: Online Harassment]. These numbers are almost unchanged from 2014, when 73% reported witnessing harassment. *See* Pew Research Ctr., *supra* note 10, at 2.

[12] *See A Farewell to Comments*, Above the Law (Apr. 12, 2016), http://abovethelaw.com/2016/04/a-farewell-to-comments/ [https://perma.cc/H82M-GPVP]; *Comments*, N.Y. Times, https://www.nytimes.com/content/help/site/usercontent/usercontent.html [https://perma.cc/2B9T-PM32] (noting that "[t]he vast majority of comments are reviewed by a human moderator"); *Discussion and Submission Guidelines*, Wash. Post, https://www.washingtonpost.com/news/ask-the-post/discussion-and-submission-guidelines/?utm_vterm=.b16b9838ede7 [https://perma.cc/5PZ8-CJMP] (stating that comments by new commenters must be verified, but returning commenters are published immediately).

[13] Data & Society: Online Harassment, *supra* note 11, at 36.

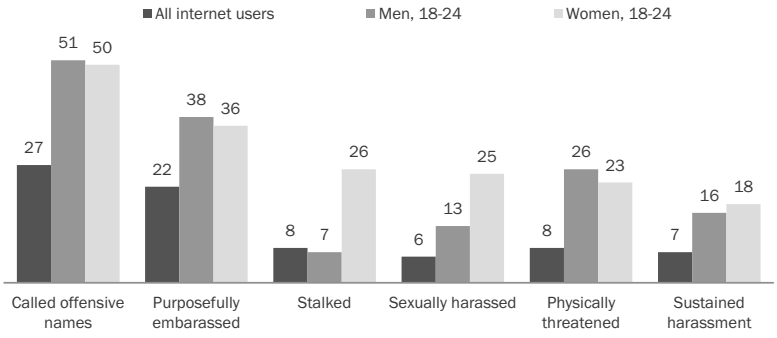
[14] Pew Research Ctr., *supra* note 10, at 2.

sexual harassment," as opposed to 13% of men aged eighteen to twenty-four and only 6% of all internet users.[15] Figures 1 and 2 from a 2014 Pew Research Center study on online harassment illustrate just how fraught a woman's online experience can be.

FIGURE 1[16]

Young women experience particularly severe forms of online harassment

Among all internet users, the % who have personally experienced the following types of online harassment, by gender and age ...



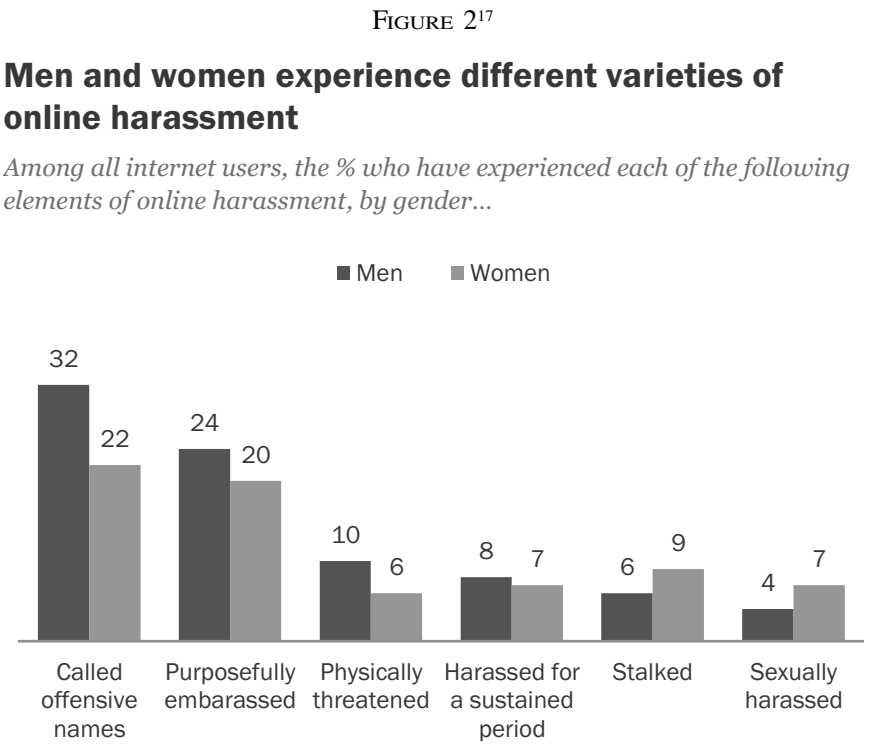
Source: American Trends Panel (wave 4).Survey conducted May 30-June 30, 2014. n=2,839.

PEW RESEARCH CENTER

[15] *Id.* at 3–4; *see also* DATA & SOCIETY: ONLINE HARASSMENT, *supra* note 11, at 36 ("Young women ages 15 to 29 bear a particular brunt of online harassment over young men and all older adults, especially direct harassment of a sexual or physical nature, or that occurs over a long period of time . . . Young people, particularly women under 30, are especially likely to be targets of cyberstalking; 14% of internet users under 30 year [sic] of age have been cyberstalked, including 20% of women under 30.").

[16] PEW RESEARCH CTR., *supra* note 10, at 4.

FIGURE 2[17]



The rise of social media, traditionally used more by women than men,[18] is not the reason for this disproportionate harassment. Women in cyberspace have always been targeted.[19] Between 2000 and 2008, 72.5% of cyber harassment victims were women.[20] Yet if you were to search your local police department's records, you would hardly find any reports of harassment, since as few as 5% of victims report the problem to law enforcement.[21]

[17] *Id.* at 5.

[18] *See* Monica Anderson, *Men Catch up with Women on Overall Social Media Use*, PEW RESEARCH CTR. (Aug. 28, 2015), http://www.pewresearch.org/fact-tank/2015/08/28/men-catch-up-with-women-on-overall-social-media-use/ [https://perma.cc/54Q3-S6EL].

[19] *See generally* Rowena Mason, *Police and Tech Firms Are Failing to Tackle Trolling, Says Stella Creasy*, GUARDIAN (Apr. 15, 2016), https://www.theguardian.com/technology/2016/apr/15/online-trolling-not-taken-seriously-enough-labour-stella-creasy [https://perma.cc/UNK3-4EHJ].

[20] Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 379 (2009).

[21] PEW RESEARCH CTR., *supra* note 10, at 6.

Academia also reflects the disparate concern of men and women. The website Journalist's Resource collected a "research review" of papers discussing internet harassment and online threats in 2015: of ten first-named authors on twelve papers, nine are women.[22]

b. Economic Impact

At the moment a threat is received, a victim's first concern is their safety. As the harassment continues, the steps the victim takes to protect themself can cause a significant economic impact, re-victimizing that person. Some costs are easily quantified, such as "legal fees, online protection services, and missed wages,"[23] with an average cost to the victim of $1,200.[24] Others are harder to measure, such as business opportunities lost when clients fear that they will be targeted if they hire a victim.[25] And, though difficult to assess, there is an opportunity cost to the time required to build the necessary paper trail—to prove stalking and harassment, to get police to pay attention, or to identify the perpetrator after a successful attack. One victim described spending "countless hours" over four years "logging the online activity of one particularly committed cyberstalker, "just in case" he carried out his threats."[26]

i. Lost Business Opportunities

It is relatively easy to measure the economic impact of harassment on journalists in online media, and their stories provide a good introduction to the problem. Over 43% of female journalists responding to a 2013 survey by the International Women's Media Foundation work in online media, and that percentage has presumably increased in the past three years.[27] Out of 921 respondents, 138 reported "[i]nsults or criticism published online," and ninety-one reported threats of violence against them.[28] The effect of such harassment goes far beyond the personal impact on the journalists, who are "concerned for their personal security and in some instances [become] depressed and experience[ ] psychological trauma."[29] Some women adopted

---

[22] *Internet Harassment and Online Threats Targeting Women: Research Review*, JOURNALIST'S RESOURCE, http://journalistsresource.org/studies/society/gender-society/internet-harassment-online-threats-targeting-women-research-review [https://perma.cc/73BE-A9B6] (last updated July 13, 2015).

[23] Hess, *supra* note 1.

[24] Representative Katherine Clark, Address at Harvard Law School (Apr. 11, 2016).

[25] *See* 2016 Claire Interview, *supra* note 3; Rothkopf, *supra* note 3.

[26] Hess, *supra* note 1.

[27] ALANA BARTON & HANNAH STORM, INT'L NEWS SAFETY INST. & INT'L WOMEN'S MEDIA FOUND., VIOLENCE AND HARASSMENT AGAINST WOMEN IN THE NEWS MEDIA: A GLOBAL PICTURE 7 (2014), http://newssafety.org/uploads/IWMF.FINALA.pdf [https://perma.cc/K35U-HHWL].

[28] *Id.* at 10.

[29] *Id.* at 13.

pseudonyms, and some dropped stories out of fear for their own safety, while others stopped reporting from certain regions or moved away, and sometimes left journalism entirely.[30] Nor is this reaction limited to women, although the gender difference is noticeable: 27% of all Americans self-censored on the internet in 2016, but for women under thirty years old that figure was 41%.[31] These figures and stories illustrate the economic impact of harassment on individuals and on the field as a whole. Not only are global perspectives muzzled as journalists respond to harassment by writing less, but the disproportionate impact of online harassment on women means that some stories, which can only be told by women, are never shared.[32]

On the business development side, online harassment campaigns can cause a different kind of negative economic impact by excluding victims from fora where critical contacts are made. For example, at South by Southwest, a technology event where over 40,000 people participate in industry conferences and trade shows,[33] publicity can be key to launching a new business. South by Southwest success stories include Twitter and Foursquare,[34] but two panel discussions about gaming at the 2015 event, one about online harassment and one about "the current social/political landscape in the gaming community," were cancelled without notice to the participants after the event organizers received "numerous threats of on-site violence."[35]

Significant business opportunities are also lost if women who have been harassed follow all-too-frequent suggestions to limit their public exposure online, by making their accounts private and otherwise refraining from engaging in the social life of the internet. In fact, 26% of victims of online

---

[30] *See id.* at 13–14. Specifically, online-only harassment was responsible for some of these outcomes: "Respondents said that the use of harassment online is sometimes effective in silencing them and their colleagues. A Canadian respondent said she rarely does online journalism after facing numerous threats and insulting comments through digital platforms. A journalist from Argentina said she writes online under a pseudonym to avoid abuse." *Id.* at 15; *see generally id.* at 14–15.

[31] DATA & SOCIETY: ONLINE HARASSMENT, *supra* note 11, at 4.

[32] *See, e.g.*, Lynsey Addario, *It's What I Do*, N.Y. TIMES: LENS (Mar. 30, 2011), https://lens.blogs.nytimes.com/2011/03/30/lynsey-addario-its-what-i-do/ [https://perma.cc/24UV-39C2]. Addario, a war photographer, stated, "Women offer a different perspective. We have access to women on a different level than men have . . . . In the Muslim world, most of my male colleagues can't enter private homes. They can't hang out with very conservative Muslim families. I have always been able to. . . . I've always found it a great advantage, being a woman."

[33] *See* SXSW, ANALYSIS OF THE ECONOMIC BENEFIT TO THE CITY OF AUSTIN FROM SOUTH BY SOUTHWEST 2 (2015), https://www.sxsw.com/wp-content/uploads/2016/05/2015-sxsw-economic-impact-analysis.pdf [https://perma.cc/7S5E-EXMG].

[34] *See* Sarah Kessler, *6 Successful SXSW Startup Launch Stories*, MASHABLE (Mar. 5, 2011), http://mashable.com/2011/03/05/sxsw-launches/#n2vJJgJOHaq8 [http://perma.cc/8WYQ-47S9].

[35] Nick Wingfield, *SXSW Cancels Gamer Panels After Threats*, N.Y. TIMES: BITS (Oct. 26, 2015, 8:40 PM), http://bits.blogs.nytimes.com/2015/10/26/sxsw-cancels-gamer-panels-after-threats/?_r=0 [https://perma.cc/M69E-J2XS]; Caroline Sinders, *I Was on One of Those Canceled SXSW Panels. Here Is What Went Down.*, SLATE (Oct. 29, 2015, 4:33 PM), http://www.slate.com/articles/double_x/doublex/2015/10/sxsw_canceled_panels_here_is_what_happened.html [https://perma.cc/YHA5-PH62].

harassment disconnect their social media, internet, or phone.[36] But as harassment victim Lenora Claire put it, "I'm a casting producer, I cast reality shows. I can't do that. I get hired because I have this huge social media reach, if I'm casting a show I put a call out to my 18,000 people on Twitter . . . . I can't just turn my social media off."[37]

The economic impact of a persistent online stalker, as shown by the experience of Lenora Claire, who promotes her various jobs online, is far-reaching. Claire's stalker "cost her a modeling job with L'Oreal" by "bombard[ing]" YouTube videos of her makeup tutorials with threats so consistently that she was dropped from the contract "because they didn't want to deal with it."[38] Claire has also lost out on new job opportunities, both known and unknown, due to her stalker's blog (and other internet postings) threatening her and her associates with rape and violence.[39] The threats of violence are so pervasive that "even her good friends are reluctant to recommend her for various jobs because they know that he could easily flood anything posted on the internet with violent comments, or target others for choosing to associate with Claire."[40]

Damage to professional relationships is another form of economic harm. Claire works as a freelance casting producer, and her relationship with a casting company was imperiled when her stalker sent a death threat to her boss.[41] The threat read: " 'Do not continue to pursue any kind of relationship with Lenora Claire or we will kill you. . . . If you continue to pursue a relationship or social influence over Lenora you will be killed.' "[42] Claire's strong five-year relationship with her boss helped her keep her job after the first round of threats, even after her boss considered the expense of hiring security.[43] At the time, Claire stated, "If I was in any other circumstance, as a freelancer, I would not be brought back, and I would lose my job. They're willing to let people go for far less."[44] However, as the threats continued, and Claire's stalker showed up at the workplaces of some of his other stalking victims,[45] Claire's boss was no longer willing to take the risk.[46] Claire only received a show to cast when her stalker was jailed, and as soon as he

[36] DATA & SOCIETY: ONLINE HARASSMENT, *supra* note 11, at 5.
[37] 2016 Claire Interview, *supra* note 3.
[38] *Id.*
[39] *See id.*
[40] Rothkopf, *supra* note 3, at 1. R
[41] 2016 Claire Interview, *supra* note 3; Rothkopf, *supra* note 3 at 1. R
[42] Rothkopf, *supra* note 3, at 1. R
[43] *See* 2016 Claire Interview, *supra* note 3.
[44] *Id.*
[45] As Claire put it, "He went to a woman's office in Silicon Valley, walked up to the front desk, and he said 'Hi, I'm Superman, and I'm here to rape Christine.' " The police were called, and served a temporary restraining order on him, but did not arrest him. Telephone Interview with Lenora Claire (March 1, 2017) (hereinafter 2017 Claire Interview).
[46] "I had never gone more than a month without working for that man, in five years, but he didn't bring me back for a year. It wasn't technically fired, [because he let me finish out the show I was working on], but he didn't bring me back." *Id.*

was freed the work stopped, "validating [her] claim that [her boss] liked [her] work but didn't like the threat of everyone dying."[47] (Claire's stalker, Justin Massler, was arrested by the Secret Service one block away from Trump Tower in December 2016 for violating the restraining order Ivanka Trump had against him).[48]

Because of this online harassment, it has become "problematic for people to hire" Claire, since before any public appearance she "has to tell the owners to hire extra security, because [her stalker] made threats to [her] there," and "a lot of people don't want that extra pain in the ass."[49] Claire has since sold a television show aimed at helping other harassment victims, with episodes focusing on how to get restraining orders, track IP addresses, and more.[50]

ii. Swatting

The economic harm caused by online harassment is not necessarily limited to an individual; some perpetrators choose to afflict an entire community by wasting public resources on fake emergencies (a practice known as "swatting").[51] Swatting, or the act of calling SWAT teams to respond to a fake emergency at the victim's house, is a tactic "often used to harass journalists, academics, domestic violence survivors and celebrities."[52] Not only does the victim suffer the surprise and fear of having heavily armed officers raid their home, but it is common practice for SWAT officers to shoot any dogs they find on the premises; as a result, many swatting victims lose beloved pets.[53] In addition to the emotional distress inflicted on the victim, each swatting costs a police department anywhere from $1,500 to $100,000 in taxpayer funds depending on how many first responders mobilize (for the

[47] *Id.*

[48] *See id.*; *see also* Jenni Miller, *Secret Service Arrests Ivanka Trump's Stalker*, N.Y. MAG.: CUT (Dec. 10, 2016), http://nymag.com/thecut/2016/12/ivanka-trumps-stalker-arrested-by-secret-service.html [http://perma.cc/U6FD-F9YT].

[49] 2016 Claire Interview, *supra* note 3.

[50] *See* 2017 Claire Interview, *supra* note 45.

[51] "The action or practice of making a prank call to emergency services in an attempt to bring about the dispatch of a large number of armed police officers to a particular address." *Swatting*, OXFORD DICTIONARIES, https://en.oxforddictionaries.com/us/definition/swatting [https://perma.cc/A27R-CUZY].

[52] AP, *Massachusetts Congresswoman Fighting "Swatting" Calls Falls Victim to One*, MASSLIVE (Feb. 1, 2016, 9:34 PM), http://www.masslive.com/news/index.ssf/2016/02/Massachusetts_congresswoman_fi.html [https://perma.cc/PA4P-DE9X].

[53] *See* Dan Marcou, *Dealing with Dogs on SWAT Operations: 10 Tactical Options*, POLICE-ONE.COM (Nov. 4, 2014), https://www.policeone.com/use-of-force/articles/7774893-Dealing-with-dogs-on-SWAT-operations-10-tactical-options/ [https://perma.cc/72FX-2DFU]; *see also* Matt Weinberger, *A Woman Who Was Threatened with Death (and Worse) for a Year Explains How to Protect Against Online Harassment*, BUSINESS INSIDER (Mar. 4, 2015, 9:46 PM), http://www.businessinsider.com/zoe-quinn-gamergate-developer-how-to-protect-yourself-2015-3 [http://perma.cc/LXM8-S7UC].

more expensive calls, more than seventy may respond).[54] Representative Katherine Clark of Massachusetts has sought to address this issue by sponsoring the Interstate Swatting Hoax Act,[55] "which would make it a federal crime to spur an emergency response by any law enforcement agency without cause" and would focus on requiring the convicted perpetrator to pay restitution to police for the cost of the response as long as no deaths result.[56] However, only a few months after introducing the Act, Clark was herself swatted despite warning police that it was a possibility.[57]

iii. Doxxing

Another economically harmful practice associated with online harassment is "doxing" or "doxxing," defined as "the callous and careless exposure of a private life for no purpose whatsoever"[58] by "[s]earch[ing] for and publish[ing] private or identifying information about (a particular individual) on the Internet, typically with malicious intent."[59] One organization has allegedly coordinated a group doxxing attempt.[60] Doxxing has an economic impact both when the victim takes expensive preventative measures and when the publication of private information is followed by more harassment or threats. The impact can be quite severe, as when victims are forced to flee their homes and remain in undisclosed locations, unable to return to their workplaces or continue their regular work schedule.[61]

---

[54] *See* Ben Johnson, *Swatting: Not a New Phenomenon, But the Cost Is Rising*, MARKETPLACE (May 19, 2015, 5:00 AM), http://www.marketplace.org/2015/05/19/tech/swatting-not-new-phenomenon-cost-rising [https://perma.cc/X374-NA46] (reporting standard costs of $1,500 to $3,000, but rising to $15,000 in one town); Alan Gathright, *"Swatting" Hoax Cost $25,000 for Law Enforcement Response to Bogus Hostage Incident in Greeley*, DENVER 7 NEWS (June 15, 2015, 1:41 PM), http://www.thedenverchannel.com/news/front-range/greeley/swatting-hoax-cost-25000-for-law-enforcement-response-to-bogus-hostage-incident-in-greeley [https://perma.cc/86WR-NH37] (reporting costs of $25,000 for a swatting incident at a community college in Colorado that drew 58 law enforcement personnel from seven police departments across the county, and reporting that "an April 2014 swatting incident in Long Beach, New York cost about $100,000" because more than 70 people responded from multiple police departments).

[55] Interstate Swatting Hoax Act, H.R. 4057, 113th Cong. (2015).

[56] Joshua Miller, *Police Swarm Katherine Clark's Home After Apparent Hoax*, BOS. GLOBE (Feb. 1, 2016), https://www.bostonglobe.com/metro/2016/02/01/cops-swarm-rep-katherine-clark-melrose-home-after-apparent-hoax/yqEpcpWmKtN6bOOAj8FZXJ/story.html [https://perma.cc/N73G-7TAS].

[57] *See* Representative Katherine Clark, Address at Harvard Law School (Apr. 11, 2016).

[58] C.S-W., *What Doxxing Is, and Why it Matters*, ECONOMIST: ECONOMIST EXPLAINS (Mar. 10, 2014), http://www.economist.com/blogs/economist-explains/2014/03/economist-explains-9 [https://perma.cc/YFG5-H5J4].

[59] *Dox*, OXFORD DICTIONARIES, https://en.oxforddictionaries.com/definition/dox [https://perma.cc/W2U9-A67S].

[60] Lenora Claire stated that the MRA [Men's Rights Association] put her on a "rape list" and tried to doxx her, but she cleared all of her information from search websites (like PeopleFinder) and got a P.O. box, and they were not able to find her address. 2017 Claire Interview, *supra* note 45.

[61] *See, e.g.*, Keith Stuart, *Brianna Wu and Human Cost of Gamergate: "Every Woman I Know in the Industry Is Scared,"* GUARDIAN (Oct. 17, 2014, 2:02 PM), https://www.theguar

III. Current Law

a. Divergent State Law

In every state, it is a crime to stalk or harass another person. But state laws vary widely regarding whether and to what extent specific provisions for *online* stalking or harassment are included.[62] Cyberbullying statutes are generally used only when the victim is a minor and generally envision that the perpetrator is also a minor and are therefore outside the scope of this Note.[63] The question of whether and how to update the statutes for the modern age is being answered differently in different states. Some states fail to mention electronic communication at all, while other states have enacted legislation specifically addressing harassment perpetrated through electronic and digital communication.

Nebraska, for example, was singled out in a 2013 paper qualitatively analyzing cyber stalking and cyber harassment legislation in the United States as the "one exception . . . that makes no specific reference to electronic or digital communication" in its statutes.[64] The Nebraska statute on stalking and harassment stated in 2013 that acts of "stalking the person or telephoning, contacting, or otherwise communicating with the person" were forbidden, but did not expressly indicate that electronic communications were included.[65] In January 2015, a bill was proposed to amend that law, removing "stalking the person" and adding "including communicating by electronic means" to the end of the sentence.[66] However, in the time since then, no action has been taken on the bill except one committee hearing and a carryover to the new legislative session, and the old version is up to date as of March 2, 2017.[67] Therefore, Nebraska remains an outlier.

On the opposite end of the spectrum are those states which have enacted statutes specific to online harassment. Arkansas, for example, has a

dian.com/technology/2014/oct/17/brianna-wu-gamergate-human-cost [https://perma.cc/X5FC-FVB2] ("Brianna Wu doesn't know when she can go home again. She can't tell me where she is—doing so might not be safe. Last Friday, her personal details were pasted on the chat forum, 8chan. Within minutes she was receiving sickening threats. . . . She said to her husband, 'we've got to get out of here.' They called the police; the police agreed.").

[62] *See* Steven Hazelwood & Sarah Koon-Magnin, *Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis*, 7(2) Int'l J. Cyber Criminology 155, 160 tbl.1 (2013); *see also State Cyberstalking and Cyberharassment Laws*, Nat'l Conf. State Legislatures, https://web.archive.org/web/20130522144712/http://www.ncsl.org/issues-research/telecom/cyberstalking-and-cyberharassment-laws.aspx [https://perma.cc/66JL-DUQY] (last updated Nov. 16, 2012).

[63] *See, e.g.*, 18 Pa. Cons. Stat. § 2709(a.1) (2016) (reciting the crime "cyber harassment of a child" and articulating punishments only for juveniles).

[64] Hazelwood & Koon-Magnin, *supra* note 62, at 159 (citing Neb. Rev. Stat. § 28-311.02 (2017)).

[65] Neb. Rev. Stat. § 28-311.02.

[66] Leg. Neb. 307, 104th, 1st Sess. (Neb. 2015).

[67] *See id.*; Neb. Rev. Stat. § 28-311.02 (2017).

statute entitled "Unlawful computerized communications" (which, interestingly, is found in the "offenses against property" subtitle).[68] In Arkansas:

> [a] person commits the offense of unlawful computerized communications if, with the purpose to frighten, intimidate, threaten, abuse, or harass another person, the person sends a message: . . . On an electronic mail or other computerized communication system with the reasonable expectation that the other person will receive the message and in that message threatens to cause physical injury to any person or damage to the property of any person.[69]

This crime is a misdemeanor and includes conduct as minor as sending an email with "obscene, lewd, or profane language."[70]

A state like Massachusetts falls somewhere in the middle, with a single statute for all types of criminal harassment that includes specific language intended to address the conduct at issue in this Note.[71] Prior to 2010, the statute defined electronic communications as "a telephonic or telecommunication device including, but not limited to, electronic mail, internet communications or facsimile communications."[72] In an apparent attempt to anticipate the invention of new methods of communication, the current version applies to harassing actions conducted using:

> a telephonic or telecommunication device or electronic communication device including, but not limited to, any device that transfers signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system, including, but not limited to, electronic mail, internet communications, instant messages or facsimile communications.[73]

An initial conviction subjects the perpetrator to imprisonment in a house of correction for no more than two and a half years, and/or to a $1,000 fine, while a second or subsequent conviction, or a prior conviction under the stalking statute, can also be punished with a state prison term of up to ten years.[74]

As this wide variation in statutory language demonstrates, the same threat can be analyzed (and perhaps prosecuted) differently state-by-state. When one state looks broadly at communication, while another focuses in on

---

[68] ARK. CODE ANN. § 5-41-108 (2015).

[69] *Id.*

[70] *Id.* §§ 5-41-108(a)(3)–(4), (b).

[71] *See* MASS. GEN. LAWS ch. 265, § 43A (2016).

[72] MASS. GEN. LAWS ch. 265, § 43A(a) (2010) (effective October 30, 2000 to May 2, 2010).

[73] MASS. GEN. LAWS ch. 265, § 43A(a) (2016).

[74] *See id.* § 43A. The stalking statute is chapter 265, § 43, which includes the same language regarding electronic communications.

intelligence transmitted by a photo optical system,[75] the average harassment victim or inexperienced prosecutor struggles.

b. Elements of the Law

As discussed in III.a., *supra*, the illegal activity at issue here goes by many names. Some states define cyberstalking as actions that cause a victim to fear "for his or her personal safety, the safety of a family member, or the destruction of property."[76] Others define it as the "repeated pursuit" of a person through "unwanted electronic communications."[77] Cyberstalking may be "threatening, coercive, or intimidating," and it "creates a sense of fear, terror, intimidation, stress or anxiety in the victim."[78] Cyberharassment is generally considered to be a broader category, covering behaviors including "threats that may be credible, profane and lewd acts, and other actions which may seriously alarm, annoy, torment, or terrorize someone, and that serve no legitimate purpose."[79]

No matter what the law is called, certain elements appear in numerous statutes and therefore served as guiding influences on the development of the model statute in Part V.a. and the Appendix, *infra*. The first element is real impact on the victim, measured as either subjective harm (whether the victim was seriously alarmed) or objective harm (whether a reasonable person would suffer emotional distress).[80] The second and third elements are re-

[75] *See id.* § 43A(a).

[76] ALICE MARWICK & ROSS MILLER, FORDHAM CTR. ON L. AND INFO. POL'Y, ONLINE HARASSMENT, DEFAMATION, AND HATEFUL SPEECH: A PRIMER OF THE LEGAL LANDSCAPE 22 (2014), http://ssrn.com/abstract=2447904 [https://perma.cc/E2ES-QLCG] [hereinafter PRIMER].

[77] Hazelwood & Koon-Magnin, *supra* note 62, at 157.

[78] *Id.*

[79] PRIMER, *supra* note 76, at 22; *see also* Hazelwood & Koon-Magnin, *supra* note 62, at 157.

[80] *See* PRIMER, *supra* note 76, at 22.

quirements of intent[81] and a course of conduct.[82] Fourth and finally, jurisdictional provisions must articulate where prosecutions can be brought.[83]

IV. Law Enforcement and Investigative Problems

a. Police Training

When the question is, "What should I do if I am a crime victim?" the answer is straightforward: "Notify local police as soon as possible and file a police report."[84] Unfortunately for victims of online harassment, there might not be a straight line from the crime to the police report. Often, local police do not consider the online harassment to be a crime, don't know what to do with the evidence or to whom they should escalate the report, or simply don't think they can do anything about "virtual" harassment.[85] Representative Clark suggests that one reason for this disconnect is that police are trained to respond to physical situations, and therefore do not recognize that online violence can be disruptive to someone's sense of safety and ability to earn a living.[86] Training materials on digital harassment are being developed, but

[81] *See id.* at 23 n.137 (noting that 30 state statutes require intent: Alabama (Ala. Code § 13A-11-8 (2017)), Alaska (Alaska Stat. § 11.61.120(a) (2016)), Arizona (Ariz. Rev. Stat. Ann. §§ 13-2916(A), 13-2921(A) (2017)), California (Cal. Penal Code §§ 422(a), 653.2(a), 653m(a)–(d) (West 2017)), Colorado (Colo. Rev. Stat. §§ 18-9-111(1), (2) (2016)), Connecticut (Conn. Gen. Stat. §§ 53a-182b(a), 53a-183(a) (2017)), Delaware (Del. Code Ann. tit. 11, § 1311(a) (2017)), Hawaii (Haw. Rev. Stat. §§ 711-1106(1), 711-1106.5(1) (2016)), Illinois (720 Ill. Comp. Stat. 5 / 26.5-1(a), 5 / 26.5-3(a)(1)–(3) (2016)), Indiana (Ind. Code § 35-45-2-2(a) (2016)), Iowa (Iowa Code § 708.7(a) (2017)), Kansas (Kan. Stat. Ann. §§ 21-6206(a)(1)(B)–(D) (2017)), Maine (Me. Rev. Stat. Ann. tit. 17-A §§ 506(1)(B)–(D) (2017)), Maryland (Md. Code Ann., Crim. Law § 3-805(b)(1)(i) (West 2017)), Minnesota (Minn. Stat. § 609.795 subdiv. 1(3) (2016)), Mississippi (Miss. Code Ann. §§ 97-29-45(1)(a)–(d) (2017)), New York (N.Y. Penal Law § 240.30 (McKinney 2017)), North Dakota (N.D. Cent. Code § 12.1-17-07(1) (2017)), Oklahoma (Okla. Stat. tit. 21, §§ 1172(A)(2)–(4) (2017)), Oregon (Or. Rev. Stat. § 166.065(1) (2016)), Pennsylvania (18 Pa. Cons. Stat. § 2709(a) (2016)), South Carolina (S.C. Code Ann. §§ 16-3-1700(B), 16-17-430(A)(2),(5) (2016)), South Dakota (S.D. Codified Laws § 49-31-31(1)–(4) (2017)), Tennessee (Tenn. Code Ann. § 39-17-308(a) (2016)), Texas (Tex. Penal Code Ann. §§ 33.07(a)–(c) (West 2015)), Utah (Utah Code Ann. § 76-9-201(2) (West 2016)), Vermont (Vt. Stat. Ann. tit. 13, §§ 1027(a), (b) (2017)), Virginia (Va. Code Ann. § 18.2-152.7:1 (2016)), West Virginia (W. Va. Code § 61-3C-14a(a) (2016)), and Wisconsin (Wis. Stat. §§ 947.0125(2)(a)–(f) (2017)).

[82] *See id.* at 23 (citing Neb. Rev. Stat. Ann. § 28-311.02).

[83] *See id.* (citing Mich. Comp. Laws § 750.411s (2015); Miss. Code Ann. § 97-29-45 (2017)).

[84] *See What Should I Do if I Am a Crime Victim?*, State Bar of Cal., http://www.calbar.ca.gov/Public/Pamphlets/CrimeVictim.aspx#1 [https://perma.cc/HK3W-9L77].

[85] *See generally* Rebecca Watson, *Why I Don't Just Go To The Cops*, Skepchick (Oct. 10, 2013), http://skepchick.org/2013/10/why-i-dont-just-go-to-the-cops/ [https://perma.cc/NF8U-6P6Q]; 2016 Claire Interview, *supra* note 3.

[86] Representative Katherine Clark, Address at Harvard Law School (Apr. 11, 2016).

they are aimed at "intermediate-level detectives," not at the beat cops who arrive at your house when you call the police.[87]

Police should take reports of violent online harassment seriously, especially because there is "a positive and significant relationship between communicated threats and violence risk."[88] A 2016 study of online harassment found that 12% of online harassment victims reported that the perpetrators also attempted to harm them in person; this translates to 3% of all Americans.[89] To prevent this harm, best practices for initial police intervention include delivering an official warning to the offender and "explaining the law and policy."[90] Of course, if the perpetrator is unfamiliar and anonymous, the perpetrator must first be identified before the police could deliver their warning.

The stories of two women, Rebecca Watson and Lenora Claire, illustrate the types of difficulties faced by even the most technologically savvy victims of online harassment who seek the prosecution and conviction of the perpetrator. In each woman's case, the perpetrator was initially a stranger, but both victims were eventually able to locate and identify the perpetrators.

Rebecca Watson is a digital journalist who runs the feminist science blog Skepchick.org.[91] The first threat she received, shortly after starting the website, was via email: "If I lived in Boston I'd put a bullet in your brain"; she was able to identify the man's state from his IP address and reported the situation to the Boston police.[92] However, the police response was extremely unhelpful, as Watson recounted: "They told me there wasn't much they could do because he apparently lived in another state. They offered to take down a report, but admitted that nothing would come of it unless someone one day put a bullet in my brain."[93]

Next, after a reader of her website discovered a "website of a man who had written disturbing things about murdering women in general and [Watson] in particular, including photos of [Watson] with targets on them," Watson asked other readers of her website to assist with the investigation, and she was able to identify the man's name, age, and location.[94] She then

---

[87] Press Release, FBI, [*FBI, Partners, Offer Online Cyber Training for Law Enforcement First Responders*] (Oct. 19, 2016), https://www.fbi.gov/news/stories/online-cyber-training-for-law-enforcement-first-responders [https://perma.cc/5MZV-GHVQ].

[88] *See* J. Reid Meloy, *Stalking and Violence*, *in* STALKING AND PSYCHOSEXUAL OBSESSION: PSYCHOLOGICAL PERSPECTIVES FOR PREVENTION, POLICING, AND TREATMENT 106, 117 (Julian Boon & Lorraine Sheridan eds., 2002).

[89] DATA & SOCIETY: ONLINE HARASSMENT, *supra* note 11, at 24. These numbers are twice as high for women under 30 (6%). *Id.* at 26.

[90] NAT'L CTR. FOR VICTIMS OF CRIME, U.S. DEP'T OF JUSTICE OFFICE OF CMTY. ORIENTED POLICING SERVICES, STALKING 22 (Jan. 2004), http://www.popcenter.org/problems/pdfs/stalking.pdf [https://perma.cc/B5QX-W9A4].

[91] *Author Archive: Rebecca Watson*, SKEPCHICK, https://skepchick.org/author/rebecca/ [https://perma.cc/GC25-U3UL].

[92] Watson, *supra* note 85.

[93] *Id.*

[94] *Id.*

called the man's local police department, who "told [her] there was nothing they could do and that [she]'d have to make a report with [her] local police department."[95] After calling her own local police department, she was transferred through several phone lines before reaching someone who "told [her] that there was nothing they could do but take a report in case one day 'Rick' followed through on his threats, at which point they'd have a pretty good lead."[96] Watson is still alive, and she no longer updates the "Page O' Hate" of screenshots of the threats against her, but that certainly doesn't mean that the perpetrators have been prosecuted and convicted.[97]

Lenora Claire's personal experiences with online harassment, discussed in Part II.b.i., *supra*, also illustrate the difficulties victims face in prosecuting their harassers. In 2011, when Claire was working as an art curator, she met a stranger at a gallery opening.[98] The man informed her that he would stalk her and, true to his word, he has done so ever since.[99]

Claire has been documenting all of the abuse, which ranged from "rapey" to death threats to fake Google accounts impersonating her and posting offensive statements.[100] She knew that restraining orders only worked if you could find the perpetrator and serve them, and her stalker was homeless, so she didn't go to the police.[101] After four years of daily harassment, Claire's stalker threatened to kill her boss, so Claire decided to try to report it.[102] "[She] walked in [to the LAPD] with a mountain of evidence, both online, handwritten letters, everything, going 'OK, I have death threats, rape threats, he has entire blogs dedicated to raping me,'" and "they belittled [her], which [she] was really surprised about."[103] She spoke to four LAPD officers who "shuffled [her] around, . . . kept [her] there for six hours," and took no action besides photocopying the handwritten letters and instructing her to file a report.[104] When Claire asked police if they would track her stalker's IP address so she would know if he was in California, they refused, and when she "asked them, 'what are some of the safety measures [she] could be taking,' . . . they offered [her] nothing."[105]

Claire summed up her initial experience with the police as follows: "I just thought that if you were getting a credible threat from someone with a

---

[95] *Id.*

[96] *Id.*

[97] Rebecca Watson, *Page O' Hate*, SKEPCHICK, http://skepchick.org/page-o-hate/ [https://perma.cc/4GYL-AA74] (last updated Sept. 22, 2014).

[98] 2016 Claire Interview, *supra* note 3.

[99] *Id.* Complicating Claire's situation is the fact that her stalker is homeless, is schizophrenic, and moves around frequently. It is very difficult to serve a restraining order on him because he contacts her from a variety of public locations, including public libraries and Apple stores. *Id.*

[100] *Id.*

[101] 2017 Claire Interview, *supra* note 45.

[102] 2016 Claire Interview, *supra* note 3; Part II.b.i., *supra*.

[103] 2016 Claire Interview, *supra* note 3.

[104] *Id.*

[105] *Id.*

confirmed violent history that maybe [the police] would at least hear you out, and take some effort to do something, but they did absolutely nothing."[106] The police "did not understand the ramifications of someone creating a Google account to impersonate" Claire, which left her feeling like she was "speaking to an older, out-of-touch person who didn't understand why [she] was in such a panic."[107]

In both cases, the women were harassed to the point where each feared that threats of death, serious bodily injury, or sexual assault were viable and danger was imminent. But the police simply didn't take them seriously, evincing a philosophy that "abuse has proliferated to the point of meaninglessness."[108] The police may have felt that reporters and other online personalities shouldn't take death threats seriously because the "assertions are entirely toothless,"[109] or because threats are merely "bullying."[110] This trivialization of harassment leads directly to "underenforcement of criminal law."[111] Victims don't report the harassment to authorities because they are afraid they won't be taken seriously, and the law-enforcement agencies "refuse to pursue cyber harassment complaints on the grounds that the conduct is legally insignificant."[112] This result might also be affected by the lack of training in cyberlaw.[113] As Watson's story exemplifies, police "are often either incapable of properly investigating harassment or unwilling to do so until it has traveled offline."[114]

Training materials exist to fix these specific problems, and will be addressed in more detail in Part V.c, *infra*. A police officer who thinks usernames are "secret codes" and doesn't "seem to know what an IP address" is fails the citizens who rely on law enforcement to keep them safe from fear and danger.[115]

---

[106] *Id.*

[107] *Id.*

[108] Hess, *supra* note 1.

[109] *Id.* (quoting Jim Pagels, *Death Threats on Twitter Are Meaningless. You Should Ignore Them.*, SLATE (Oct. 30, 2013), http://www.slate.com/blogs/future_tense/2013/10/30/twitter_death_threats_are_meaningless_you_should_ignore_them.html [https://perma.cc/68E8-6T45]).

[110] *Id.* (quoting Jen Doll, *Welcome to the Twisted Age of the Twitter Death Threat*, ATLANTIC (Nov. 27, 2012), https://www.theatlantic.com/technology/archive/2012/11/welcome-twisted-age-twitter-death-threat/321111/ [https://perma.cc/T8TA-UQKC]).

[111] Citron, *supra* note 20, at 402.

[112] *Id.*

[113] *Id.*

[114] *Id.* at 402 n.234.

[115] Hess, *supra* note 1.

b. Investigative Resources

As the National White Collar Crime Center noted, "it is still difficult for law enforcement to track and prosecute perpetrators."[116] From a law enforcement perspective, a great deal more resources, time, and technical ability are required to track down an anonymous internet attacker, who could be physically located anywhere in the country, or even in the world, than to investigate a threat issued in the same city as the victim. Victims with sufficient resources can hire private investigators, but in nearly every category of harassment, those most harassed have a household income of under $30,000 per year.[117] A victim in that income bracket might struggle to afford a P.O. box that would protect their address. For most victims, $95/hour for a private investigator is definitely not in the budget,[118] and those victims rely on their city and state law enforcement to protect them.

No uniform jurisdictional or investigative structure applies to every state; some state attorneys general have both the jurisdiction and the resources to investigate violent online harassment, while other states delegate those tasks to state bureaus of criminal investigation or city district attorneys. For example, only twelve states have dedicated Cyber Crime Divisions in their state attorney general's offices.[119] An additional eighteen have Internet Crimes Against Children Divisions, digital evidence laboratories, or some other mechanism for prosecuting online crimes against children (though not adults).[120] Some states, such as Washington, lack original criminal jurisdiction and therefore suggest that all internet crimes be reported to the Internet Crime Complaint Center,[121] an FBI unit that focuses on internet fraud (but not explicitly threats of violence).[122] When local police do not know how to handle a cyber threat, whether or not a victim obtains justice depends entirely on the victim's home state.

---

[116] NAT'L WHITE COLLAR CRIME CTR., CYBERSTALKING (MARCH 2015) 1 (Mar. 2015), http://www.nw3c.org/docs/research/cyberstalking.pdf?sfvrsn=8 [https://perma.cc/G8X8-MQ9L].

[117] DATA & SOCIETY: ONLINE HARASSMENT, *supra* note 11, at 25–26.

[118] *How Much Does a Private Investigator Cost?*, THUMBTACK, https://www.thumbtack.com/p/private-investigators-cost [https://perma.cc/DLL2-J7YR] (last updated Mar. 1, 2017).

[119] Arkansas and others. *See, e.g.*, *Cyber Crimes*, ARK. ATTORNEY GENERAL OFFICE, https://arkansasag.gov/public-safety/cyber-crimes/ [https://perma.cc/TP99-R8FP].

[120] Arizona and others. *See, e.g.*, *Internet Crimes Against Children Task Force*, ARIZ. ATTORNEY GENERAL OFFICE (2017), http://azicac.org/ [https://perma.cc/ASQ5-BNJZ].

[121] *Internet Crime*, WA. STATE OFFICE OF THE ATTORNEY GEN., http://www.atg.wa.gov/internet-crime [https://perma.cc/E6YZ-JA7X] ("While the Washington State Attorney General's Office . . . can fight Internet crime through our high-tech unit using the state's Consumer Protection Act, when it comes to other types of crimes, our efforts are limited by the office's lack of original criminal jurisdiction. If you are a victim of an internet crime, we encourage you to contact IC3.").

[122] *IC3 Mission Statement*, FBI INTERNET CRIME COMPLAINT CTR. (IC3), http://www.ic3.gov/about/default.aspx [https://perma.cc/V8SW-LF3G].

The law enforcement agency with the most investigative resources is the FBI. While its jurisdiction extends nationwide,[123] it generally does not focus on investigating online harassment. For example, the mission of the Internet Crime Complaint Center (IC3) is for the public to be able to report "Internet-facilitated criminal activity,"[124] but the IC3 lists only white collar frauds as examples of internet crime.[125] Similarly, online harassment is not listed among the key priorities of the Cyber Crime Division of the FBI.[126]

c. Prosecutorial Jurisdiction

Victims of online harassment who are targeted by unfamiliar perpetrators and want to get a restraining order face the immediate barrier of service, regardless of whether a statute explicitly criminalizes online harassment. In many states, a restraining order, protective order, or injunction against harassment (the names vary) can be obtained even without the defendant's address.[127] In a jurisdiction that requires a course of conduct for a harassment conviction, a protective order can be the best proof of the severity and timing of the initial threats. However, the order is not valid unless and until it is served on the defendant; if the victim cannot identify or locate her harasser, she cannot serve him with the protective order.[128]

As discussed in Part III.b, *supra*, most states do not articulate their jurisdictional requirements for online harassment cases, and even a state that discusses jurisdiction may hesitate to grant it. For example, Michigan makes prosecution of online perpetrators easy, even if the victim does not know where the perpetrator was at the time the offending message was sent—which could be the case with either familiar or unfamiliar perpetrators. A perpetrator can be prosecuted in Michigan for the crime of "[p]osting messages through [an] electronic medium without consent" as long as the victim was in Michigan at the time the threat was sent, or if the perpetrator knew that the victim was a Michigan resident.[129] In Mississippi, on the other

---

[123] *See* 18 U.S.C. § 875(c) (2012).

[124] *IC3 Mission Statement*, *supra* note 122.

[125] *Frequently Asked Questions*, FBI INTERNET CRIME COMPLAINT CTR. (IC3), http://www.ic3.gov/faq/default.aspx [https://perma.cc/6XKB-UDDR] ("Q: How does the IC3 define Internet crime? A: . . . Internet crime involves the use of the Internet to communicate false or fraudulent representations to consumers. These crimes may include, but are not limited to, advance-fee schemes, non-delivery of goods or services, computer hacking, or employment/business opportunity schemes.").

[126] *Cyber Crime*, FBI, https://www.fbi.gov/about-us/investigate/cyber [https://perma.cc/DQ9B-RE9G].

[127] *See, e.g.*, *Domestic Violence (Family Offense)*, N.Y. COURTS, https://www.nycourts.gov/courts/nyc/family/faqs_domesticviolence.shtml#op3 [https://perma.cc/W33J-D4YJ].

[128] *See, e.g.*, ARIZ. REV. STAT. ANN. § 12-1809(J) (2016) ("A copy of the petition and the injunction shall be served on the defendant within one year from the date the injunction is signed. An injunction that is not served on the defendant within one year expires. The injunction is effective on the defendant on service of a copy of the injunction and petition and expires one year after service on the defendant.").

[129] MICH. COMP. LAWS ANN. § 750.411s(7) (West 2016).

hand, a person can be prosecuted for the crime of "Obscene electronic and telecommunications" only in the Mississippi county in which the communication originated.[130] The relevant statute declares that if "the call, conversation or language originates outside of the State of Mississippi then such person shall be prosecuted in the county to which it is transmitted."[131] This requirement means that a Mississippi victim who wants a prosecution to be brought in their own county must first prove that the perpetrator was either in their county or not in Mississippi at all. This requires information—namely the perpetrator's exact physical location at the moment the threat was sent—that can be impossible to obtain for an unfamiliar perpetrator.

This mismatch means that victims in some states are more protected than victims in other states. Prosecutors in Michigan and similar states can always exercise their discretion and decline to prosecute an out-of-state perpetrator. But Mississippi victims may feel pressure to perform a thorough investigation on their own before a prosecutor can help. This requirement can chill crime reporting.[132]

V. SOLUTION

a. Proposed Legislation

This Note proposes a two-tiered model state statute to address some of the problems discussed in Part III, *supra*. The statute is split into first-degree and second-degree crimes, with first-degree online harassment focused on the more serious threats such as death or rape and second-degree online harassment aimed at less severe but persistent threats that cause substantial emotional distress. An intent of recklessness is required, and provisions exist for both a course of harassing conduct and for a single instance of aggravated harassment. Jurisdiction exists in the states where the perpetrator lives, or where the perpetrator was present at the time he committed the act; and in the states where the victim lives, or where she was present at the time she received the threat. It is important to note in the statute that even anonymous communication is criminalized so that future developments in related laws, such as those governing the service of protective orders, will be easily transferred to this statute.

First-degree online harassment focuses on the types of violent threats that have appeared in nearly all of the individual stories recounted in this Note. Threats of death, serious bodily injury, and sexual assault, aimed at a victim or a member of the victim's family or household, are felonies. "Sex-

[130] MISS. CODE ANN. § 97-29-45(6) (West 2016).

[131] *Id.*

[132] *See, e.g.*, 2017 Claire Interview, *supra* note 45. Claire was stalked for four years before she reported the crime to police because she knew she didn't have enough information to get a restraining order. *Id.*

ual assault" and "serious bodily injury" are not defined because it is assumed that each state will already have definitions for those terms. These are the most serious crimes, the ones that cause people to move out of their homes,[133] obtain restraining orders,[134] cancel public speaking engagements,[135] and lose business from employers and friends who are terrified that they will be next.[136] Classification as a felony is necessary to guide state law enforcement into taking these cases seriously.

Second-degree online harassment is classified as a misdemeanor in order to increase the conviction rate. If a perpetrator sends one tweet that he will break a victim's arm and another that he will break her windows, but he lives 200 miles away, prosecutors would probably be unwilling to charge him with a felony. Therefore, it is necessary to have the option of a less serious charge in order to create a criminal record of convictions and to prove a pattern of harassing behavior. Depending on the state, this might even be a fineable rather than a jailable offense; either way, the important result is that the perpetrator's record is available to future victims as proof that their concern is legitimate.

However, if a person who is convicted of second-degree online harassment has a previous online harassment conviction or a prior felony conviction involving the same victim, then the charge would be increased from misdemeanor to felony. This provision is aimed at serial stalkers and domestic abusers. One of the purposes of punishment is incapacitation, and especially if misdemeanors are punishable by fines rather than jail time, this grading requirement may be the only way for victims of continuing harassment to get peace of mind.

The mens rea requirement in this model statute is recklessness. The existing federal cyberstalking statute requires "the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate."[137] This is a higher standard than the one proposed here, but it is balanced out by the federal statute's lower threshold for what qualifies as an act, as any course of conduct that a) used a facility of interstate commerce and b) "would be reasonably expected to cause substantial emotional distress to a person" qualifies.[138] The model statute proposed here has more complicated act requirements, in order to remain squarely in the "true threat" exception to the First Amendment.

True threats "communicate a serious expression of an intent to commit an act of unlawful violence," even if the speaker did not actually intend to

---

[133] *See* Stuart, *supra* note 62.

[134] *See* Elonis v. United States, 135 S. Ct. 2001, 2006 (2015).

[135] *See* Saeed Ahmed & Tony Marco, *Anita Sarkeesian forced to cancel Utah State speech after mass shooting threat*, CNN (Oct. 15, 2015, 10:57 AM), http://www.cnn.com/2014/10/15/tech/utah-anita-sarkeesian-threat/ [https://perma.cc/MD3M-2QLN].

[136] *See* 2016 Claire Interview, *supra* note 3.

[137] 18 U.S.C. § 2261A(2) (2012).

[138] *Id.* § 2261A(2)(B) (2012).

carry out the threat.[139] The purpose of the true threat exception is to protect individuals from "the fear of violence," from "the disruption that fear engenders," and from "the possibility that the threatened violence will occur."[140] Intimidation, "where a speaker directs a threat to a person or group of persons with the intent of placing the victim in fear of bodily harm or death," is the conduct most frequently at issue in cases of first-degree violent online harassment, and "is a type of true threat."[141]

The question of what mens rea is necessary for an online communication to constitute a true threat was addressed in *Elonis v. United States*.[142] In that case, Elonis was indicted by a grand jury for violating 18 U.S.C. § 875(c), which "makes it a crime to transmit in interstate commerce 'any communication containing any threat . . . to injure the person of another.' "[143] At issue were multiple threats Elonis made on his Facebook page in the form of rap lyrics, including threats to murder his wife, to shoot up a kindergarten, and to kill the FBI agents who came to his house to investigate the kindergarten threat.[144] At his trial, the jury was instructed that " '[a] statement is a true threat when a defendant intentionally makes a statement in a context or under such circumstance wherein a reasonable person would foresee that the statement would be interpreted by those to whom the maker communicates the statement as a serious expression of an intention to inflict bodily injury or take the life of an individual.' "[145] Elonis was convicted under this negligence standard, and the Third Circuit affirmed.[146] However, the Supreme Court held that "negligence is not sufficient to support a conviction," because "[f]ederal criminal liability generally does not turn solely on the results of an act without considering the defendant's mental state."[147] The Court concluded that a mens rea of knowledge would certainly satisfy the statutory requirements, and declined to "be the first appellate tribunal" to address recklessness.[148]

In an opinion concurring in part and dissenting in part, Justice Alito stated that the "Court's disposition of this case is certain to cause confusion and serious problems" because of its refusal to address the recklessness standard.[149] Alito defined "reckless conduct as morally culpable" and would hold "that a defendant may be convicted under [online threat statutes] if he

---

[139] Virginia v. Black, 538 U.S. 343, 359–60 (2003).

[140] *Id.* at 360 (quoting R.A.V. v. City of St. Paul, 505 U.S. 377, 388 (1992)).

[141] *Id.*

[142] 135 S. Ct. 2001 (2015).

[143] *Id.* at 2004, 2007 (quoting 18 U.S.C. § 875(b) (2012)).

[144] *See id.* at 2005–2007.

[145] *Id.* at 2007 (quoting United States v. Elonis, 897 F. Supp. 2d 335, 341 n.5 (E.D. Pa. 2012)).

[146] *See id.*

[147] *Id.* at 2012–13.

[148] *Id.* at 2013. Justice Alito concurred in part and dissented in part. Justice Thomas dissented, reading in a general intent requirement and declining to extend further First Amendment protection to threats.

[149] *Id.* at 2013 (Alito, J., concurring in part and dissenting in part).

or she consciously disregards the risk that the communication transmitted will be interpreted as a true threat."[150] Because "[n]othing in the Court's non-committal opinion prevents lower courts from adopting that standard," and for the reasons discussed above, this Note adopts recklessness as the appropriate standard of mens rea.[151]

The test for whether the threat is a "true threat," and therefore actionable by law enforcement rather than protected by the First Amendment, is the reasonable person standard. "[T]he term 'threat' in [online threat statutes] can fairly be defined as a statement that is *reasonably* interpreted as 'an expression of an intention to inflict evil, injury, or damage on another.' "[152] Some people are more easily frightened than others; for example, women who are digital journalists might develop thick skins as a result of high exposure to online harassment,[153] at least if they stay in the business. The same threatening words would cause different levels of alarm if directed at different victims, such as a college media intern or an experienced blogger. A reasonable person standard levels the playing field.

This Note advocates for a statute that strikes a balance between the interests of free speech and the interests of victims. The word "imminent" differentiates between an act which would fall into the course of conduct requirement—which alone would be insufficient for a conviction—and an act of aggravated harassment. If the act would place a reasonable person in fear (for first-degree) or inflict substantial emotional distress on a reasonable person (for second-degree) that act is necessary but not sufficient for a conviction. There must be a second act to establish a course of conduct. For example, an email reading "I will kill you" for first-degree, or "You are unqualified and only have your job because you slept your way to the top" for second-degree might be a malicious venting of feelings, rather than a true threat, from a perpetrator who is hundreds of miles away and has no intention of actually killing the victim. In that case, further conduct would be necessary to cross the bar of the First Amendment and ensure that the statute is not overbroad.

However, sometimes a single threat is enough to constitute an act of aggravated harassment. Such a threat would cause a reasonable person to believe that they would be killed, seriously injured, or sexually assaulted (for first-degree) or that they would be injured or have their property seriously damaged (for second-degree) in the very near future. Proximity is implicated in imminence but is not de facto necessary. For example, a tweet directed at

---

[150] *Id.* at 2015–16 (Alito, J., concurring in part and dissenting in part).

[151] *Id.* at 2016 (Alito, J., concurring in part and dissenting in part).

[152] *Id.* at 2014 (Alito, J., concurring in part and dissenting in part) (emphasis added).

[153] *See generally This American Life: If You Don't Have Anything Nice to Say, SAY IT IN ALL CAPS*, CHI. PUBLIC RADIO (Jan. 23, 2015), http://www.thisamericanlife.org/radio-archives/episode/545/if-you-dont-have-anything-nice-to-say-say-it-in-all-caps?act=1 [https://perma.cc/9UE8-M66W] (Act One, *Ask Not For Whom The Bell Trolls; It Trolls for Thee*, telling the story of writer Lindy West and one of her trolls).

Brianna Wu stating, "This means I have to hunt for WU now" and accompanied both by a picture of Wu clearly taken earlier that day by someone in a crowd about twenty feet away, captioned "I took a pic earlier," and by commentary that the photographer "COULDA WENT IN FOR THE KILL" would constitute aggravated first-degree harassment.[154] An act of aggravated second-degree harassment might be an email implying close enough physical proximity that the perpetrator is capable of carrying out the threat immediately if he is not stopped, such as "You are unqualified and only have your job because you slept your way to the top. I am going to slice your face up so it never happens again, but I won't stain your polka dot shirt." An image of a pile of assault weapons, bullets engraved with the victim's name, and a Google Earth image of the victim's home does not imply proximity, but does indicate imminence, and would therefore be an act of aggravated first-degree harassment.

The purpose of the jurisdictional language in subsection four is twofold. First, it clarifies "who is legally in charge of investigating and prosecuting the act," to prevent crimes from going unpunished.[155] Second, it permits the state with the most resources to bring charges, so that victims in smaller or less well-funded states are not necessarily foreclosed from justice. For example, if a Massachusetts perpetrator harassed a Maine victim, then either Maine or Massachusetts could press charges, which would allow the victim to access the resources of the Cyber Crime Division of the Massachusetts Attorney General's Office. (Maine does not have a dedicated cybercrime division.) Similarly, if an Alabama perpetrator took a cross-country road trip and sent threatening emails to the Maine victim from Alaska, California, Colorado, Georgia, and Florida, the victim would be able to use California's cybercrime resources to prosecute the case.[156] This Note recognizes that this proposal is politically difficult because of the free-riding problem of states without cybercrime resources pressuring the taxpayers of Massachusetts, California, and the other states with a focus on cybercrime. This problem is exacerbated if the additional prosecutions cause an increase in state taxes or in the length of time it takes to prosecute a case. One possible solution is the creation of a National Evidence Laboratory, as discussed in Part V.b, *infra*, which would take care of all the evidentiary aspects of the prosecution and make it possible for smaller states to prosecute cases of online harassment. Another outcome might be that the rhetoric of being tough on cybercrime proves so politically popular that politicians in states without cybercrime resources choose to create them, levelling the playing field for victims..

---

[154] Brianna Wu (@Spacekatgal), TWITTER (Mar. 7, 2015, 1:01 PM), https://twitter.com/spacekatgal/status/574313995345223680 [https://perma.cc/3XD5-FXE9] (retweeting @ChumsKnifeblade and @SST_Demonik).

[155] *See* Hazelwood & Koon-Magnin, *supra* note 62, at 165–66.

[156] *California Cyber Crime Center*, CA. ATTORNEY GENERAL OFFICE, https://oag.ca.gov/c4 [https://perma.cc/XXY4-9SWN].

b. National Evidence Laboratory

Currently, those cases severe enough to be escalated up to the FBI, such as the Brianna Wu case, are prosecuted under the federal threat and cyberstalking statutes, which can use the interstate commerce clause to sweep away all jurisdictional barriers.[157] Most cases don't meet that high threshold, however, and while some states have digital evidence laboratories to process seized electronics and unlock the evidence hidden on a phone or hard drive, most do not.

Simply put, sifting through large amounts of data requires fast computers. Due to economies of scale in terms of processing power and the expense of the specialized equipment necessary to pull the data out of technology, which is constantly changing,[158] smaller states become more efficient and cost-effective when they pool their resources. A national evidence laboratory would offer not only technicians and equipment but also well-established relationships with various tech companies—at least in terms of standardized subpoenas and contacts for service.

In order to conserve resources, the national evidence laboratory would offer its services only to state prosecutors pursuing first-degree online harassment cases. The second-degree cases would be left to the uneven resources and imperfect enforcement mechanisms of the states. Investigating online harassment cases can require an enormous investment of time, on the order of hundreds of hours per case,[159] so the national resources should be reserved for the types of cases most likely to escalate to real physical harm.

c. Training Materials

Currently, the best source of training materials is the National Cyber Crime Conference, but its materials are not widely available. The National Cyber Crime Conference is an annual event designed to "educate law enforcement . . . and prosecutors on ways to investigate . . . and ultimately prosecute cases involving digital evidence" in a world where the "ability to obtain, analyze and understand digital evidence . . . has become essential to law enforcement."[160] At the 2015 conference, police and prosecutors could attend lectures on "What the H#ck is a Hashtag," as well as "Becoming an

---

[157] 18 U.S.C. §§ 875(c), 2261A(2) (2012).

[158] For example, in order to access data from old devices, a digital evidence laboratory must have a cable for every plug. Storing these cables takes an entire wall of the Massachusetts laboratory.

[159] *See generally* Jeanne Hayes, *Forensic Testing Turnaround Times in 50 States* tbl.6 (Conn. General Assembly OLR Research Report No. 2010-R-0086, Feb. 17, 2010), https://www.cga.ct.gov/2010/rpt/2010-R-0086.htm [https://perma.cc/FJ8J-9EJ2].

[160] 2016 NCCC ATTENDEE JUSTIFICATION, MASS. ATTORNEY GENERAL, http://www.mass.gov/ago/docs/nccc/nccc-justification.pdf [https://perma.cc/Y2YZ-639R].

Internet Super Sleuth – Google it!" and "All Things Facebook."[161] While higher-level lectures constituted the bulk of the conference,[162] the fact that these introductory lectures were included in a conference limited to law enforcement professionals who paid a $350 registration fee may indicate both how widespread the problem of police ignorance is and that the solution to the problem already exists. Such training materials clearly need to be more widely available, rather than limited to those who attend in person. The FBI is slowly beginning to make online training materials available, but as of early 2017, there are very few resources.[163]

One remedy for the dearth of easily accessible training materials was recently proposed by Representative Katherine Clark of Massachusetts. The Cybercrime Enforcement Training Assistance Act that she proposed may have had almost no chance of passage,[164] but it provides an excellent template for what a nationally organized, state-level training system should be. The purpose of the bill is "to make grants to States and units of local government for the prevention, enforcement, and prosecution of cybercrimes against individuals, and for other purposes."[165] The materials are directed at state and local law enforcement personnel; state and local prosecutors, judges, and judicial personnel; and state and local emergency dispatch personnel.[166] The grants discussed in the bill are intended to train these personnel to "identify and protect victims of cybercrimes against individuals," "utilize Federal, State, local, and other resources to assist victims of cybercrimes against individuals," "identify and investigate cybercrimes against individuals," and "enforce and utilize the laws that prohibit cybercrimes against individuals."[167]

Despite its title, the bill goes farther than the provision of specific training materials. Funds are directed at the enforcement of "laws that prohibit cybercrimes against individuals," such as the model statute proposed in this Note.[168] Funds are also earmarked for public education, the establishment of

---

[161] *Conference Agenda*, 2015 National Cyber Crime Conference, http://docplayer.net/16381817-2015-national-cyber-crime-conference-monday-april-27-2015-conference-agenda-day-1.html [https://perma.cc/GUV9-F5BX]. Other lectures potentially relevant to this Note include "Social Media Investigations," "Search Warrants for Digital Evidence in the Cloud," "IP Tracing: Where on the Internet is that Host System?" "What's New in Social Media," "The Role of Online Social Media ODINT in Predicting and interdicting Spree Killings," "Utilizing Social Media in your Investigations," "Social Media and Legal Documentation," "Online Terrorism of Women in the Tech Industry," and "Digital & Multimedia Evidence Legal Considerations." *Id.*

[162] *See id.*

[163] Press Release, FBI, *supra* note 87.

[164] GovTrack gives the Cybercrime Enforcement Training Assistance Act of 2016, H.R. 4740, a 4% chance of getting past committee and a 1% chance of getting enacted. GovTrack, https://www.govtrack.us/congress/bills/114/hr4740 [https://perma.cc/9VCP-64QY].

[165] *See* H.R. 4740, 114th Cong. (Mar. 15, 2016), https://www.gpo.gov/fdsys/pkg/BILLS-114hr4740ih/pdf/BILLS-114hr4740ih.pdf [https://perma.cc/WTN4-LR2X].

[166] *Id.* §§ 2(c)(1)–(3).

[167] *Id.* §§ 2(c)(1)–(4).

[168] *Id.* § 2(c)(4).

cybercrime task forces, the establishment or enlargement of digital forensics laboratories, the expenses involved in extraditing offenders from one state to another, and the transfer of "expertise and information" from federal to state law enforcement agencies.[169] This last provision is particularly important, because realistically only one resource, the FBI, exists for victims in the states with no state-level cybercrime division and the states with no state-level resources devoted to the prosecution of cybercrimes in any way.

Ultimately, the best long-term solution is some form of nationally accessible, centrally standardized set of training materials, similar to the materials proposed in the Cybercrime Enforcement Training Assistance Act. In the short term, while legislatures debate the appropriate funding levels for these training centers, the simplest solution is to make the materials from the National Cyber Crime Conference more widely available to law enforcement personnel and to require refresher courses on technology and developments in laws relating to cybercrimes.

VI. Conclusion

For some internet users, violent online harassment is inescapable. The economic impact is severe. From individual costs, such as legal fees and lost job opportunities, to societal costs, such as suppression of diverse opinions in cyberspace and the impact on taxpayers of repeated swatting attacks, harassment takes its toll. But the three-pronged solution proposed in this Note should alleviate some of this harm.

First, the model statute discussed in Part V.a, *supra*, addresses the problem of divergent state laws. The mens rea of recklessness strikes a balance between the free speech rights of those negligent people who did not intend to cause harm and those who meet the higher threshold of knowledge. The felony/misdemeanor split between first-degree and second-degree online harassment gives prosecutors more options. Finally, by broadening the scope of prosecutorial jurisdiction, the statute would give victims the flexibility to seek justice in locations with more resources.

Second, a national evidence laboratory would provide economies of scale. Since each investigation can be quite time-consuming, the laboratory would conserve resources by investigating only first-degree crimes as those are most likely to escalate to real physical harm.

Finally, standardized and improved training of law enforcement officials and prosecutors is essential for this new system to flourish. The Cybercrime Enforcement Training Assistance Act proposed by Representative Clark is a good framework for the long term, but unfortunately, it stalled in committee. In the short term, accessibility to the training materials of the National Cyber Crime Conference should be greatly expanded, and law enforcement officers should be required to keep their knowledge up to date.

[169] *Id.* §§ 2(c)(5)–(9).

Many other professions require re-certification and courses of study to keep skills sharp; law enforcement should as well.

Some people will always take advantage of the ability to harass, stalk, and threaten others from behind the protection of anonymity and a computer screen. An updated criminal code reflecting that reality and associated training and logistical support will help online harassment victims find justice and peace.

VII. Appendix

Model Statute for Online Harassment

(a) A person is guilty of the crime of online harassment in the first degree if
   1. The person intended, knew, or consciously disregarded a substantial and unjustifiable risk that the words or conduct described in subsection (2) would place a person in reasonable fear of death, serious bodily injury, or sexual assault;
   2. The person used electronic communication, anonymously or otherwise, to threaten to sexually assault, or cause death or serious bodily injury to another person or member of that person's family or household; and
   3. The act(s) were either:
      i. Part of a pattern of conduct or series of two or more acts within a period of time; or
      ii. Sufficiently grave that a single act suffices to place a reasonable person in imminent fear of death, serious bodily injury, or sexual assault.
   4. The accused may be prosecuted for all acts against a victim in any county in which any single act described in subsection (2) was committed, or where the actor or victim resides.
   5. Any person convicted of violating section (a) is guilty of a felony.

(b) A person is guilty of the crime of online harassment in the second degree if
   1. The person intended, knew, or consciously disregarded a substantial and unjustifiable risk that the words or conduct described in subsection (2) would alarm the recipient and would cause a reasonable person to suffer substantial emotional distress;
   2. The person used electronic communication, anonymously or otherwise, to threaten
      i. To cause bodily injury to another person or member of that person's family or household; or
      ii. To cause serious damage to the property of another person; and
   3. The act(s) were:
      i. Part of a pattern of conduct or series of two or more acts within a period of time; or
      ii. Sufficiently grave that a single act suffices to place a reasonable person in imminent fear of bodily injury or serious property damage.
   4. The accused may be prosecuted for all acts against a victim in any county in which any single act described in subsection (2) was committed, or where the actor or victim resides.

5. Except as provided in subsection (6) of this section, any person convicted of violating section (b) is guilty of a misdemeanor.
6. Any person convicted of violating section (b) is guilty of a felony if:
   i. The person has a prior conviction under such section or a substantially conforming criminal violation; or
   ii. The person has been convicted of any felony in this state or has been convicted of a crime in another jurisdiction which, if committed in this state, would constitute a felony and the victim or a family or household member of the victim was also the victim of such previous felony.