University of Maryland Law Journal of Race, Religion, Gender and Class

Volume 17 | Issue 1 Article 8

An Old Crime in a New Context: Maryland's Need for a Comprehensive Cyberstalking Statute

Christie Chung

AN OLD CRIME IN A NEW CONTEXT: MARYLAND'S NEED FOR A COMPREHENSIVE CYBERSTALKING STATUTE

Christie Chung*

INTRODUCTION

The Department of Justice defines stalking as a "pattern of repeated and unwanted attention, harassment, contact, or any other course of conduct directed at a specific person that would cause a reasonable person to feel fear."[1] Unlike a multitude of other crimes, stalking is unique in that it is a composite offense made up of a pattern of, oftentimes, varied behaviors.[2] These behaviors include, but are by no means limited to: direct and indirect threats of harm, following or lying in wait for the victim at their home, place of work, and other frequented locales, and sending unwanted gifts and items.[3]

Although the first anti-stalking statute was not passed until 1990, rapid technological advances in the intervening decades have entirely redefined the scope of the offense.[4] As a "borderless medium" that provides a veneer of anonymity, the internet has proven to be a fertile landscape of new opportunity for those looking to stalk, harass, or otherwise attack others.[5] Cyberstalking, as a subset of computer-

* J.D. Candidate 2018, University of Maryland Francis King Carey School of Law; B.A., 2015, University of Maryland College Park. The author thanks her parents, Lillian Wong and Vinh Chung, her siblings, Amy Chung Wilson and William Chung, and her friend, Joanne Ly, for their lifelong support and encouragement. The author is also grateful to those special teachers over the years who have taught her the value of hard work, dedication, and community engagement.

[1] *Stalking*, U.S. DEP'T OF JUST., https://www.justice.gov/ovw/stalking (last updated Jan. 6, 2016).

[2] *See id.* Stalking can be defined as "a course of conduct directed at a specific person that involves repeated visual or physical proximity, nonconsensual communication, or verbal, written or implied threats, or a combination thereof, that would cause a reasonable person fear." PATRICIA TJADEN & NANCY THOENNES, NAT'L INST. JUST., U.S. DEP'T. OF JUST., STALKING IN AMERICA: FINDINGS FROM THE NATIONAL VIOLENCE AGAINST WOMEN SURVEY 2 (Apr. 1998), https://www.ncjrs.gov/pdffiles/169592.pdf. *See also infra* Part III.B.

[3] *Stalking*, *supra* note 1 (linking to *Stalking Resource Center*, NAT'L CTR. FOR VICTIMS OF CRIME, http://victimsofcrime.org/our-programs/stalking-resource-center (last visited Apr. 18, 2017)).

[4] *See* Naomi H. Goodno, *Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 MO. L. REV. 125, 127, 129 (2007).

[5] *Id.* at 129.

related crimes, occurs when perpetrators utilize information technology infrastructures (*i.e.* cyberspace) to carry out the conventions of physical stalking.[6]

This Comment maintains that the current state of Maryland's criminal law leaves cyberstalking victims with questionable and uncertain means of recourse. In establishing a body of law that befits the seriousness of cyberstalking as a potential precursor to violent crime, the State should create a statute tailored to the crime of cyberstalking instead of relying on traditional stalking and harassment laws that do not work in the cyber context. Specifically, the formulated law needs to articulate clear *actus reus* and *mens rea* standards that adequately balance free speech concerns with the needs and experiences of victims.[7]

Part I of this Comment provides a profile of the victims against whom cyberstalking is often perpetrated.[8] This examination of the victims provides a central framework through which subsequent discussion of the crime and reform measures should be situated. Part II of this Comment differentiates cyberstalking from traditional stalking and assesses how these differences inform the process of investigating, prosecuting, and convicting offenders.[9] Part III and Part IV contemplate the sufficiency of current federal and Maryland statutes, respectively.[10] Finally, Part V addresses the identified deficiencies in existent statutes and submits a draft cyberstalking statute for adoption in the state of Maryland.[11]

[6] *See generally* Marlisse S. Sweeney, *What the Law Can (and Can't) Do About Online Harassment*, THE ATLANTIC (Nov. 12, 2014), http://www.theatlantic.com/technology/archive/2014/11/what-the-law-can-and-cant-do-about-online-harassment/382638 (exploring the dark side of cyberspace and the variety of interpersonal communications that take place therein).
[7] *See infra* Part V.C.
[8] *See infra* Part I.
[9] *See infra* Part II.
[10] *See infra* Part III–IV.
[11] *See infra* Part V.

I. CONTEXTUALIZING CYBERSTALKING THROUGH THE PRISM OF VICTIM EXPERIENCES

Although stalking is a gender-neutral crime in that both men and women are victimized, the majority of victims are disproportionately female.[12] Unsurprisingly, this gendered dimension of traditional stalking has carried over into virtual perpetration of the crime.[13] Working to Halt Online Abuse, a nonprofit organization founded in 1997, reported that 72.5 percent of their incident reports between 2000 and 2007 originated from women.[14] Moreover, women are not only more likely to be stalked online, the harassment they encounter is more likely to be gender-based.[15] That is, while men are more likely to be called "offensive names," or be "purposefully embarrassed," the harassment women face online often stems from the fact that *they are women*, and is more likely to be sexual in nature.[16] Without a doubt, men and women are both subjected to harassment online;[17] however, acknowledgement of how the harassment differs

[12] SHANNAN CATALANO, STALKING VICTIMS IN THE UNITED STATES–REVISED, OFFICE OF JUST. PROGRAMS, U.S. DEP'T OF JUST. 1 (Sept. 2012), http://www.bjs.gov/content/pub/pdf/svus_rev.pdf. In a study of 220,995,170 individuals over a 12-month period, 2.2% of females experienced stalking as compared to 0.8% of males. *Id.* at 4.

[13] *See* Soraya Chemaly, *12 Examples: Pew's Online Harassment Survey Highlights Digital Gender Safety*, HUFFINGTON POST, http://www.huffingtonpost.com/soraya-chemaly/pew-online-harassment-survey_b_6028350.html (last updated Dec. 22, 2014) ("Women are much more likely to experiencing [sic] stalking, sexual harassment and sustained harassment online."); *see also* Amanda Hess, *Why Women Aren't Welcome on the Internet*, PAC. STANDARD (Jan. 6, 2014), https://psmag.com/why-women-aren-t-welcome-on-the-internet-aa21fdbc8d6#.u9qphnlna. According to a 2006 study conducted by the University of Maryland, "[a]ccounts with feminine usernames incurred an average of 100 sexually explicit or threatening messages a day. Masculine names received 3.7." *Id.*

[14] Danielle Keats Citron, *Civil Rights in Our Information Age*, in THE OFFENSIVE INTERNET: PRIVACY, SPEECH, AND REPUTATION 32 (Saul Levmore & Martha C. Nussbaum eds., 2010); *Working to Halt Online Abuse*, http://www.haltabuse.org (last visited Apr. 18, 2017).

[15] *See* Chemaly, *supra* note 13 (arguing that women not only experience more severe forms of cyber harassment, but that the harassment stems from a deeply rooted culture of misogyny).

[16] *See id.* (commenting on the quality and nature of harassment that men are more likely to endure online as compared to women).

[17] *See id.* ("Researchers found that 40 percent of Internet users report experiencing some form of online "harassment," defined in the study as name-calling, purposeful

both in form and in how it is experienced by victims will be crucial for effective legislative reform.[18]

In exploring the contours of cyberstalking by looking to its victims, it is necessary to situate cyberstalking within the context of intimate partner violence (IPV).[19] The prevalence of stalking in abusive relationships is well documented.[20] Seventy-six percent of women murdered by their intimate partners experienced a period of stalking prior to their deaths.[21] Similar to physical stalking, it is difficult to determine with absolute certainty the prevalence of cyberstalking because of underreporting.[22] That being said, in a 2009 victimization survey conducted by the Bureau of Justice Statistics, twenty-six percent of stalking victims indicated that their stalkers' pattern of conduct involved the use of technology in one form or another.[23] Notwithstanding the fact that this figure is probably, in actuality, much higher,[24] the number of stalking victims reporting the use of technology is likely only to increase in the coming years as technology continues to transform the spheres of social interaction.[25]

Society has immeasurably benefitted from modern technological advances, yet cyberspace has proven to be a regrettably fertile landscape for stalkers and abusers.[26] IPV relationships go

---

embarrassment, stalking, sexual harassment, physical threats and sustained harassment.").

[18] Goodno, *supra* note 4, at 128–33 (stating five different ways in which cyberstalking differs from traditional, physical stalking that must be taken into account for legislative reform).

[19] *See* Andrew King-Ries, *Teens, Technology, and Cyberstalking: The Domestic Violence Wave of the Future?*, 20 TEX. J. WOMEN & L. 131, 133 (2011).

[20] *See id.* at 136 (commenting on "the centrality of stalking to the domestic violence relationship and the connection between stalking and risk of physical violence.").

[21] *Id.*

[22] Donna M. Schwartz-Watts, *Commentary: Stalking Risk Profile*, 34 J. AM. ACAD. PSYCHIATRY L. 455, 455 (2006) ("Stalking remains underreported. Only one half to one third of stalking victims reported such crimes."); Michael L. Pittaro, *Cyber Stalking: An Analysis of Online Harassment and Intimidation*, 1 INT'L J. CYBER CRIM. 180, 182 (2007) (explaining how cyberstalking contributes to the "dark figure" of crime due to rampant underreporting and under-detection).

[23] King-Ries, *supra* note 19, at 133.

[24] Schwartz-Watts, *supra* note 22, at 455.

[25] *See* Pittaro, *supra* note 22, at 181.

[26] *See* Aily Shimizu, Comment, *Recent Developments: Domestic Violence in the Digital Age: Towards the Creation of a Comprehensive Cyberstalking Statute*, 28

beyond the physical component of violence; authorities characterize IPV as defined by patterns of abuse that are centrally geared towards the elimination of personal autonomy and the establishment and maintenance of control.[27] In looking at the common methods of abusers—"physical and emotional isolation, repeatedly invading the victim's privacy, supervising the victim's behavior, terminating support from family or friends, threatening violence toward the victim, threatening suicide"—it becomes abundantly clear that the internet presents new avenues of convenience and opportunity.[28] The following two excerpts illustrate the societal costs borne by the advent and commercialization of new technologies:

> A Wisconsin article reported that a woman found it impossible to escape her ex-boyfriend. He would follow her as she drove to work or ran errands. He would inexplicably pull up next to her at stoplights and once tried to run her off the highway…. The article reported that the stalker put a global positioning tracking device between the radiator and grill of the survivor's car.[29]

> In September 2001, a Michigan man was charged with installing spy software on the computer of his estranged wife. He installed a commercially available software program on her computer at her separate residence. Without her knowledge, the program sent him regular emails reporting all computer activity, including all emails sent and received and all Web sites visited.[30]

Looking at both the strong correlation between stalking and violence, and the ways in which stalkers are increasingly exploiting

---

BERKELEY J. GENDER L. & JUST. 116, 117–18 (2013) (describing the general environment of the internet as favorable to stalkers due to the anonymity and freedom from geographic constraints that it confers).

[27] King-Ries, *supra* note 19, at 135 (stating "[w]hile violence is a critical component of the relationship, the broader power and control dynamic prevails: 'The battering relationship is not about conflict between two people; rather, it is about one person exercising power and control over the other.'").

[28] *Id.*; *see also infra* Part III.

[29] Cynthia Southworth et al., *Intimate Partner Violence, Technology, and Stalking*, 13 VIOLENCE AGAINST WOMEN 842, 847 (2007).

[30] *Id*. at 848.

technological channels to interject themselves into the lives of their victims, Maryland's lack of a dedicated cyberstalking statute is an oversight that undermines the State's ability to ensure the safety and well-being of all its citizens.[31]

II. USING ELECTRONIC MEDIUMS IN PLACE OF OR IN ADDITION TO PHYSICAL SURVEILLANCE—CYBERSTALKING

The differences between physical stalking and stalking as perpetrated through electronic mediums leaves victims of cyberstalking in a precarious position. In addition to facing many of the same challenges encountered by victims of traditional stalking, victims of cyberstalking must confront the unique problems posed by cyber-based crimes.[32] Along with the consequences of potentially having their personal information compromised, victims of cyberstalking must develop strategies for addressing preservation of digital evidence, law enforcement minimalization of their sustained harms, and increased offender capabilities.[33]

A. Successful Prosecution of Cyberstalking is Frustrated by the Heavy Evidentiary Burden Carried by Victims and the Tendency to Trivialize Incidents of Cyberstalking

Victims of cyberstalking are hamstrung by the same obstacles that hinder the successful prosecution and conviction of conventional stalkers, but to a greater degree.[34] For one, stalking is one of a handful of crimes wherein the responsibility of investigation and data collection flows to victims rather than law enforcement.[35] In the absence of physical evidence or witnesses who can corroborate a

[31] *See infra* Part IV.

[32] *See generally* KRISTIN FINKLEA & CATHERINE A. THEOHARY, CYBERCRIME: CONCEPTUAL ISSUES FOR CONGRESS AND U.S. LAW ENFORCEMENT 1, CONG. RES. SERV. (2015) (outlining the complex economic, safety, and legal issues posed by "twenty-first century criminals"—that is, those who utilize the digital world to victimize).

[33] *See infra* Part II.A.–B.

[34] VIOLENCE AGAINST WOMEN GRANTS OFFICE, U.S. DEP'T OF JUST., STALKING AND DOMESTIC VIOLENCE: THE THIRD ANNUAL REPORT TO CONGRESS UNDER THE VIOLENCE AGAINST WOMEN ACT 41 (1998).

[35] *See* ANDREW KARMEN, CRIME VICTIMS: AN INTRODUCTION TO VICTIMOLOGY 380 (9th ed. 2016) (noting that the onus is on stalking victims to collect and document evidence of their victimization).

victim's allegations, it is often difficult to differentiate between "whether the contact was an act of stalking or an unintentional encounter."[36] Consequently, in many cases, "the burden of proof is so high that very few stalkers are found guilty."[37] In terms of cyberstalking, digital evidence presents its own unique set of challenges. As a repository of a tremendous amount of information, personal computers, the internet, and technology in general have rapidly become an indispensable investigative tool for victims and law enforcement alike.[38] Be it archiving incriminating e-mails or screenshotting threatening social media posts, victims may find it easier to preserve the evidence they need to build a case.[39] The problem with reliance on digital evidence stems not from its existence, however, but from its fragility and issues of accessibility.[40] The digital trail left by online activity is of little use if it is encrypted beyond recognition or remotely wiped before it can be processed.[41] Moreover, technical proficiency in activities such as encryption or hacking is no longer a limiting factor.[42] The ever-growing "services-based nature of cybercrime" allows stalkers lacking technological proficiency to nevertheless achieve their ends by purchasing the skills and services of others who do possess the requisite degree of technical expertise.[43]

---

[36] *See supra* note 34.

[37] KARMEN, *supra* note 35.

[38] *See* SEAN E. GOODISON ET AL., DIGITAL EVIDENCE AND THE U.S. CRIMINAL JUSTICE SYSTEM 1, NAT'L INST. JUST., U.S. DEP'T OF JUST. (2015), https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf (detailing how technological advances have caused major shifts in law enforcement methods for criminal investigations).

[39] *Id.* at 4.

[40] *Id.* at 7 ("Modern electronic devices…can also be fragile. As a result, digital evidence can be damaged or altered by basic actions, such as dropping an item in water, passing a powerful magnet by it, or even through sheer physical force to break components").

[41] *Id.* at 4 (noting the value of encrypting data to prevent others from accessing the content of communications between users).

[42] *See* RAJ SAMANI & FRANÇOIS PAGET, CYBERCRIME EXPOSED: CYBERCRIME-AS-A-SERVICE, MCAFEE 1, 4 (2013), http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-exposed.pdf (investigating the burgeoning underground market of services and products available for purchase or rent by potential cybercriminals).

[43] *Id.* at 4–5 (identifying the following four categories of services available to willing buyers: research (described as the sale of information concerning system vulnerabilities), crimeware (described as the "toolset" or hardware needed to conceal malware and launch attacks), cybercrime infrastructure (described as the platforms

As an aggregate crime, cyberstalking is difficult to regulate in the absence of overt misconduct on the part of the stalker.[44] In isolation, a variety of stalking behaviors may ostensibly appear insignificant or innocuous.[45] Taken in the aggregate and in the context of IPV, however, individual stalking incidents can be viewed as benchmarks of a rapidly escalating encounter between the victim and the perpetrator.[46] To the great detriment of cyberstalking victims, stalking behaviors carried out online appear particularly prone to being mischaracterized or trivialized.[47] Citing a study conducted by the University of Bedfordshire in which "over 60 percent of survey participants reported receiving no help from police regarding their cyber harassment complaints," University of Maryland Law professor Danielle Citron associates high rates of underreporting to the fact that "[v]ictims are uncertain as to whether [cyberstalking/harassment] is a crime or fear the police would not take them seriously."[48] The creation of a separate cyberstalking statute and its codification in Maryland's criminal law will not only provide guidance to law enforcement officers, but it will also legitimize the injuries sustained by victims as real and tangible harms.

B. The Internet has Fundamentally Transformed the Crime of Stalking—From the Identity of its Perpetrators and their Methodologies to the Harms Inflicted on Victims

Before turning to a discussion of the current state of federal and state cyberstalking laws, it is necessary to consider the scope of the crime. Generally, conventional stalking requires the stalker to be in

used to host attacks), and hacking (described as password cracking and personal information acquiring services)).

[44] *See* John B. Major, Note, *Cyberstalking, Twitter, and the Captive Audience: A First Amendment Analysis of 18 U.S.C. § 2261A(2)*, 86 S. CAL. L. REV. 117, 126 (explaining how regulation of cyberstalking is difficult given the fact that it may include acts which appear innocuous to outside observers). Stalking is less about individual actions taken against a victim and more about the cumulative harm inflicted. *See* TJADEN & THOENNES, *supra* note 2.

[45] Major, *supra* note 44, at 126–27.

[46] *Id.*

[47] DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 84 (2014) (associating the trivialization of online harassment with institutional deficiencies in the training and education of law enforcement officers).

[48] *Id.* at 21.

relatively close physical proximity to the victim.[49] In contrast, geographic boundaries are rendered irrelevant with cyberstalking as the internet provides offenders with a cheap and effective means of making direct contact with their victims.[50] Cyberspace also exposes individuals to an almost immeasurable number of potential stalkers.[51] In the current age of social media, we freely broadcast the intimate minutiae of our daily lives in a way that we would never do when confronted with strangers in the real world. The National Crime Victimization Survey reports that the vast majority (69.9%) of conventional stalkers were either intimate partners or otherwise acquainted with their victims.[52] However, when it comes to cyberstalking, research suggests that a far greater percentage of perpetrators are strangers to the victim.[53] Victims may find their ability to meet evidentiary burdens further frustrated and fears compounded by this anonymous facet of online interactions.[54]

Perpetrators will find that they are limited only by their imaginations in utilizing technology to harass and surveil. Common techniques employed by cyberstalkers include sending unsolicited hateful, obscene, or otherwise threatening e-mails *en masse*, posting personal or fictitious information about the victim, impersonating the victim, and soliciting the participation of third parties.[55] Individuals

[49] *See* Shimizu, *supra* note 26, at 117–18 (commenting on how geographic boundaries are a nonfactor in the commission of cyberstalking).
[50] *Id.*
[51] For example, Twitter has 313 million active daily users. COMPANY, https://about.twitter.com/company (last visited Apr. 18, 2017). Facebook surpassed one billion users in 2015. Facebook, FACEBOOK (Aug. 27, 2015), https://www.facebook.com/facebook/videos/vb.20531316728/10154009776186729/?type=2&theater.
[52] CATALANO, *supra* note 12, at 5.
[53] BONNIE S. FISHER & JOHN J. SLOAN, CAMPUS CRIME: LEGAL, SOCIAL, AND POLICY PERSPECTIVES 247 (3rd ed. 2013).
[54] *See* Adrienne Lafrance, *When Will the Internet be Safe for Women?*, THE ATLANTIC (May 20, 2016), https://www.theatlantic.com/technology/archive/2016/05/when-will-the-internet-be-safe-for-women/483473. Congresswoman Katherine Clark, who has been a victim of pernicious cyber harassment because of her legislative efforts to reform cyberstalking and harassment laws, explains, "You do internalize it, and even though it is not someone directly in front of you, there is something about the anonymous nature of it—when you don't know where a threat is coming from—that really gets into someone's psyche." *Id.*
[55] Sweeney, *supra* note 6.

will need to adopt an increasingly proactive approach to cybersecurity as "[d]atabases of personal information available on the Internet can enable a stalker to trace a victim's…real name, address, telephone number, and other personal information."[56] In the first successful conviction of an offender under a state's cyberstalking law, a California man was convicted after he impersonated his victim in various chat rooms and solicited others to visit the victim at her house to act out so-called "rape fantasies."[57] On at least six different occasions, men appeared at the victim's house—sometimes in the middle of the night—and offered to rape her.[58] The disturbing facts of this case are not unique, and in a number of other cases, have resulted in the rape and violent assault of women.[59]

In many ways, modern technology has completely revolutionized the capabilities of stalkers.[60] With global positioning systems (GPS), spyware software,[61] keystroke loggers,[62] and hidden

[56] TRUDY M. GREGORIE, CYBERSTALKING: DANGERS ON THE INFORMATION SUPERHIGHWAY, NAT'L CTR. FOR VICTIMS OF CRIME 3 (2001), http://victimsofcrime.org/docs/src/cyberstalking---dangers-on-the-information-superhighway.pdf?sfvrsn=2.
[57] *Id.*
[58] *Id.*
[59] *See* Caroline Black, *Ex-Marine Jebidiah James Stipe Gets 60 Years for Craigslist Rape Plot*, CBS NEWS (June 29, 2010, 1:30 PM), http://www.cbsnews.com/news/ex-marine-jebidiah-james-stipe-gets-60-years-for-craigslist-rape-plot (discussing a case in which a man posed as his ex-girlfriend on Craigslist, which led to her being raped at gunpoint); *see also* Sarah Larimer, *Woman Uses Craigslist "Rape Fantasy" Ads to Target Her Ex's Wife, Authorities Say*, WASH. POST (July 20, 2016), https://www.washingtonpost.com/news/morning-mix/wp/2016/07/20/woman-uses-craigslist-rape-fantasy-ads-to-target-her-exs-wife-authorities-say/?utm_term=.aabe9c4fd178 (discussing a case in which a woman posed as her husband's ex-girlfriend on Craigslist, causing the ex-girlfriend to be physically attacked in her home).
[60] *See supra* text accompanying note 26.
[61] *See Viruses, Spyware, and Malware*, MIT INFO. SYS. TECH., https://ist.mit.edu/security/malware (last visited Apr. 18, 2017) (defining spyware as "[s]oftware that surreptitiously gathers information and transmits it to interested parties. Information gathered includes visited websites, browser/system information, and your computer's IP address.").
[62] *See* Mary O. Foley, *How to Avoid Dangerous Keyloggers*, NORTON, https://us.norton.com/yoursecurityresource/detail.jsp?aid=key_loggers (last visited Apr. 18, 2017). Keystroke loggers, or keyloggers, track every key that is depressed on a computer or laptop's keyboard. *Id.* Typically used to capture sensitive information such as passwords, social security numbers, or bank accounts,

cameras, stalkers can monitor the real time movements of their victims, track all computer activities, and harvest sensitive information such as passwords and PIN numbers at their leisure and in the convenience of their own homes.[63] Similar to victims of other cybercrimes, it is difficult for victims of cyberstalking to even detect when offenders compromise their devices, privacy, and safety.[64] One example of the burgeoning risk posed by cybercriminals is Luis Mijangos, who was arrested in 2010 after the FBI discovered him using malicious software to hack into the computers of more than 200 victims.[65] Mijangos listened to the victims through their computer microphones and watched them through their webcams.[66] Of the victims, forty-four were juveniles.[67] Had Mijangos not begun blackmailing female victims with stolen sexually explicit photographs, many of these breaches would have surely remained unknown to the victims and law enforcement.[68]

From the identity of perpetrators down to the harms being inflicted on victims, advances in technology have entirely transformed

keyloggers can be transmitted as software programs or physically installed as hardware on computers. *Id.*

[63] Southworth et al., *supra* note 29, at 848–49.

[64] ADJUSTING THE LENS ON ECONOMIC CRIME: PREPARATION BRINGS OPPORTUNITY BACK INTO FOCUS 8, GLOBAL ECONOMIC CRIME SURVEY 2016, PWC (2016), http://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf (commenting on issues of detection and the trend of organizations not realizing that their networks have been compromised for extended periods of time—1 in 10 economic crimes were discovered entirely by accident.). *See also* Nate Anderson, *Meet the Men Who Spy on Women Through Their Webcams* (Mar. 11, 2013), http://www.wired.co.uk/article/webcam-spying (explaining how remote administration software gives hackers autonomous control over the computers of their victims).

[65] Richard Winton, *"Sextortion": 6 Years for O.C. Hacker Who Victimized Women, Girls*, L.A. TIMES (Sept. 1, 2011, 1:42 PM), http://latimesblogs.latimes.com/lanow/2011/09/sextortion-six-years-for-oc-hacker-who-forced-women-to-give-up-naked-pics-.html.

[66] *Id.*

[67] *Id.*

[68] *Id.* Mijangos threatened to post the intimate images and videos he found unless his female victims recorded and sent pornographic videos and images to him. *Id.* After one victim showed the treats to a friend, Mijangos posted nude photos of the victim to her Myspace page. *See id.*

the nature of stalking.[69] While legislative reform has attempted to keep pace with technological innovation, the continuously changing boundaries between cyberspace and the physical world present difficult challenges to the formulation of adequate law.[70]

III. AMBIGUITIES IN FEDERAL CYBER LAWS LEAD TO INEQUALITIES IN THE PROSECUTION OF OFFENDERS

In *Computer Crimes*, authors Fehr, LiCalzi, and Oates note that "states are often the leaders in the effort to address issues of…cyberstalking."[71] Such must be the case in Maryland because existent gaps in federal law handicap the ability of cyberstalking victims to obtain justice.

A. Conflicting Interpretations of the Interstate Communications Act Fosters Differential Access to Justice for Cyberstalking Victims

One of the key federal statutes that cyberstalking could fall under is 18 U.S.C. § 875(c), the Interstate Communications Act.[72] The statutory language of 18 U.S.C. § 875(c) states that, "Whoever 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 years, or both."[73] To secure a conviction under § 875(c), the government must successfully prove the following three elements: "(1) a transmission in interstate [or foreign] commerce; (2) a communication containing a threat; and (3) the threat must be to injure [or kidnap] the person of another."[74] With regards to cyberstalking, the first and third factor do not tend to present much issue. The second factor however raises serious issues stemming from the fact that "threat" is a term that can be subject to several constructions.

---

[69] *See supra* notes 47–54,60–63 and accompanying text.
[70] *See infra* Part III.
[71] Caroline Fehr et al., *Computer Crimes*, 53 AM. CRIM. L. REV. 977, 1018 (2016).
[72] 18 U.S.C. § 875(c) (2012).
[73] *Id.*
[74] United States v. Alkhabaz, 104 F.3d 1492, 1494 (6th Cir. 1997) (quoting United States v. DeAndino, 958 F.2d 146, 148 (6th Cir. 1992)).

The First Amendment protection of free speech does not extend to communications that convey a "true threat."[75] True threats are taken to mean "statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence."[76] In large part, internet communications pose particular First Amendment issues because the intent of users is not easily discernible.[77] Discrepancies in how various circuit courts have determined the presence or absence of *mens rea* have led to inequities in the remedies available to victims of cyberstalking.[78] Under an objective standard, the *mens rea* inquiry looks to whether a reasonable person receiving the threat would believe that it was a threat.[79] Courts that apply a more subjective standard for *mens rea* instead focus on whether a "reasonable speaker would foresee that the listener would interpret the speech as a threat of violence."[80] Differences in opinion as to the *mens rea* requirement are of tremendous importance because the standard that is applied also affects the defenses that will be available to defendants.[81] While a defendant's ability to show that he did not intend for the communication to be threatening may be determinative under a subjective standard, it would carry no weight in a jurisdiction that follows the objective standard.[82]

The facts of *United States v. Alkhabaz* are illustrative of how § 875(c)'s utility to victims of cyberstalking will fluctuate depending on

---

[75] United States v. Watts, 394 U.S. 705, 707–08 (1969).
[76] Virginia v. Black, 538 U.S. 343, 359 (2002).
[77] *See generally* Alison J. Best, Note, Elonis v. United States*: The Need to Uphold Individual Rights to Free Speech While Protecting Victims of Online True Threats*, 75 MD. L. REV. 1127 (2016).
[78] *See* Paul T. Crane, Note, *"True Threats" and the Issue of Intent*, 92 VA. L. REV. 1225, 1235–48 (2006) (surveying the differences in how lower courts have interpreted the *mens rea* requirement for determinations of "true threats"). In Elonis v. United States, 135 S. Ct. 2001, 2009 (2015), the Supreme Court held that § 875(c) must contain a *mens rea* requirement although the statute itself does not address criminal intent; ambiguities persist, however, because the Supreme Court ultimately declined to explicitly define the degree of *mens rea* needed for a conviction under the statute. Best, *supra* note 77, at 1157.
[79] Amy E. McCann, Comment, *Are Courts Taking Internet Threats Seriously Enough? An Analysis of True Threats Transmitted Over the Internet, as Interpreted in* United States v. Carmichael, 26 PACE L. REV. 523, 527–28 (2006).
[80] *Id.* at 528.
[81] Crane, *supra* note 78, at 1236.
[82] *Id.*

the jurisdiction and the particular court's interpretation of the statute's requirements. From November 1994 until approximately February 1995, the defendant in the case expressed his desire to harm women in a series of extremely sadistic e-mails with another person whom he met online.[83] The following e-mails from Alkhabaz are representative of the general nature of their communications:

> I highly agree with the type of woman you like to hurt…. I want to do it to a really young girl first. !3[sic] or 14…. There [sic] innocence makes them so much more fun--and they'll be easier to control.[84]
>
> I can't wait to see you in person. I've been trying to think of secluded spots. but [sic] my area knowledge of Ann Arbor is mostly limited to the campus. I don't want any blood in my room, though I have come up with an excellent method to abduct a bitch __ As I said before, my room is right across from the girl's bathroom. Wiat[sic] until late at night. grab [sic] her when she goes to unlock the door. Knock her unconscious. and [sic] put her into one of those portable lockers (forget the word for it). or [sic] even a duffle bag. Then hurry her out to the car and take her away…[85]
>
> Just thinking about it anymore doesn't do the trick … I need TO DO IT.[86]
>
> Alrighty [sic] then. If not next week. or [sic] in January. then [sic] definitely sometime in the Summer [sic].[87]

[83] United States v. Alkhabaz, 104 F.3d 1492, 1493 (6th Cir. 1997). Going by the name Arthur Gonda, the true identity and whereabouts of the person with whom Alkhabaz communicated remain unknown. *Id.*

[84] *Id.* at 1499 (Krupansky, J., dissenting).

[85] *Id.* at 1500 (Krupansky, J., dissenting).

[86] *Id.* at 1501 (Krupansky, J., dissenting).

[87] *Id.* Alkhabaz's e-mail was in response to a message from Gonda exclaiming, "My feelings exactly! We have to get together…I will give you more details as soon as I find out my situation…." *Id.*

Prior to these communications, Alkhabaz had also posted a number of fictitious stories online that "generally involved the abduction, rape, torture, mutilation, and murder of women and young girls."[88] In one of these stories, the victim shared the same name as one of Alkhabaz's classmates at the University of Michigan.[89]

Proclaiming to use an objective *mens rea* standard, the Sixth Circuit ruled that the communications did not constitute a threat because a reasonable person would not have taken the statements as "a serious expression of an intention to inflict bodily harm."[90] The court further read into § 875(c) a requirement that the government show *actus reus* by proving that Alkhabaz sent the e-mails for the express purpose of "effect[ing] some change or achiev[ing] some goal through intimidation."[91] Short of actually being assaulted or worse, victims will be hard pressed to meet their evidentiary burden in the Sixth Circuit if Alkhabaz's discussion of specific plans, a time frame, and even his own pronouncement that "just thinking about it anymore doesn't do the trick"[92] was not enough to show an intention to "effect some change or achieve some goal."[93] The Sixth Circuit's interpretation of § 875(c) imposed an unworkable burden on victims.

B. 18 U.S.C § 2261A(2) is Insufficiently Broad to Account for the Various Channels Through Which Cyberstalkers Reach Their Victims

In 2006, Congress amended the Federal Interstate Stalking Punishment and Prevention Act,[94] originally passed as part of the

[88] *Id.* at 1493 (stating that the stories were posted to the Usenet newsgroup "alt.sex.stories"); *see also What is Usenet?*, USENET.ORG, http://www.usenet.org (last visited Apr. 18, 2017) (describing newsgroups as the functional equivalent of modern discussion forums).
[89] Alkhabaz, 104 F.3d at 1493.
[90] *Id.* at 1496.
[91] *Id.* at 1495.
[92] *Id.* at 1501 (Krupansky, J., dissenting).
[93] *Id*. at 1496 (Krupansky, J., dissenting). Not until 2017 did the Sixth Circuit demonstrate a greater willingness to consider context when interpreting § 875(c)'s *mens rea* requirement. *See* United States v. Houston, No. 16-5007, 2017 U.S. App. LEXIS 5249, at *9, *11 (6th Cir. Mar. 23, 2017) (viewing the defendant's statements "in context," the court found that "a reasonable jury" could infer from the defendant's tone of voice an intent to cause the victim serious injury).
[94] 18 U.S.C. § 2261A (2012).

Violence Against Women Act of 1994, to specifically address cyberstalking.[95] Prior to the 2006 amendments, § 2261 was limited to actors who "with the intent to kill or injure" used the "mail or any facility of interstate or foreign commerce to engage in a course of conduct that places" another in reasonable fear of death or serious bodily harm.[96] In 2006, Congress broadened the scope of the statute to read in relevant part:

> "Whoever—
> (2) with the intent (A) to kill, injure, *harass,* . . . uses the mail, any *interactive computer service*, or any facility of interstate or foreign commerce to engage in a course of conduct that *causes substantial emotional distress* to that person . . . shall be punished as provided in Section 2261(b). (emphasis added)"[97]

Although Congress' revision of the Federal Interstate Stalking and Punishment and Prevention Act to account for cyberstalking is commendable, the statute's utility is still limited..

In *United States v. Cassidy*,[98] the District Court for the District of Maryland found § 2261A(2)(A) to be unconstitutional as applied to a defendant who used Twitter and blog postings to harass the prominent leader of a Buddhist sect in Poolesville, Maryland.[99] Cassidy served as the Sect's Chief Operating Officer for two weeks before he left following a confrontation in which it was revealed that he had misrepresented his qualifications.[100] In the months following his departure, Cassidy took to blog postings and Twitter to harass the

[95] United States v. Cassidy, 814 F. Supp. 2d 574, 581 (D. Md. 2011) ("Finally, the 2006 changes expanded the *mechanisms of injury* to add use of an "interactive computer service" to the existing list which already included use of mail or any facility of interstate or foreign commerce").
[96] *Id.* at 580.
[97] *Id.* at 580–81.
[98] *Id.* at 588.
[99] *Id*. at 576–80.
[100] *Id.* at 578. Contrary to the Sect's teachings, Cassidy was allegedly an ardent gossiper, lied about his lineage as a tulka, and falsely claimed to have had stage IV lung cancer. *Id.*

Sect.[101] The Sect maintained that "all but a few hundred of the alleged 8,000 Tweets" pertained to the church.[102]

Ultimately, the court's determination that § 2261A(2)(A) was unconstitutional as applied to Cassidy turned on First Amendment free speech protections.[103] According to the court, while "the government has a strong and legitimate interest in preventing the harassment of individuals," it was questionable whether the same interest extended to comments and communications initiated online.[104] Asserting that e-mails and phone calls were "targeted towards a particular victim and…received outside a public forum," the court found no compelling government interest in protecting individuals from the content of Tweets or blogs.[105] Crucial to its holding, the court stated that users have "the ability to 'turn off' ("block" or "unfollow") communications" and that the victim of Cassidy's defamations "had the ability to protect her 'own sensibilities simply by averting' her eyes from the Defendant's Blog."[106] The court also found the fact that the victim was "easily identifiable [as a] public figure" to be significant in that "the fundamental importance of the free flow of ideas and opinions on matters of public concern is the core of the First Amendment Protections."[107]

The court's rationale is inimical with the realities of what cyberstalking victims face. The conclusion that a victim can avoid harm simply by "averting her eyes" is an invidious misconception that diminishes the gravity of cyberstalking as a serious crime with serious—sometimes, tragic— real world consequences.[108] In

[101] *Id.* at 578–80.
[102] *Id.* The Tweets—sent by at least ten different Twitter handles all registered to Cassidy—included threats such as "want it to all be over soon sweetie?" and "Got a wonderful Pearl Harbor Day surprise for [plaintiff]…. wait for it." *Id.* at 588.
[103] Shimizu, *supra* note 26, at 126–27.
[104] Cassidy, 814 F. Supp. 2d at 585 (quoting Thorne v. Bailey, 846 F.2d 241, 243 (4th Cir. 1988)).
[105] *Id.* at 585–86.
[106] *Id.* at 578, 585 (quoting United States v. Playboy Ent. Group, 529 U.S. 803, 813 (2000)).
[107] *Id.* at 586 (quoting New York Times Co. v. Sullivan, 376 U.S. 254, 271 (1964)).
[108] *See* Black, *supra* note 59 and accompanying text; *see also* Chris Wright, *What Happened Last Fall on This Tiny New Hampshire Street Triggered a National Debate on Internet Crime. But Was the Web Really to Blame for the Death of Amy Boyer?*, BOS. PHOENIX (Aug. 10, 2000),

California's first conviction under its cyberstalking law, the victim did not even own a computer; yet, the fact that she never saw the defendant's messages made neither the terror she felt nor the men who accosted her at her home any less real.[109] The Maryland court's proffered "avert your eyes" solution is just as inappropriate and ineffective in the cyber context as it would be in any case involving a victim of conventional stalking.[110] Moreover, the Maryland court's distinction between harassment directed towards specific individuals and harassment directed towards "public figures" is anachronistic in the modern age of social media.[111] The court cited the fact that the victim had 17,221 followers on Twitter and over 143,000 views on her videos as support for finding her to be a "public figure."[112] Does a person's affinity for updating their social media channels transform them into a public figure? What of the individual whose video abruptly "goes viral" and amasses millions of views? In a day and age where anyone can be "YouTube famous"[113] or "Instagram famous,"[114]

http://www.bostonphoenix.com/archive/features/00/08/10/MURDER.html (reporting on the death of Amy Boyer, a twenty-year-old college student, who was murdered after being unknowingly cyberstalked for two and a half years. Her murderer, who was able to purchase her Social Security number and address for a little more than $150 online, chronicled his activities on a public website over the two and a half years he stalked her—"It's [actually] [obscene] what you can find out about a person on the internet," he once wrote. *Id.*).

[109] GREGORIE, *supra* note **Error! Bookmark not defined.**, at 3; Joanna L. Mishler, Comment, *Cyberstalking: Can Communication Via the Internet Constitute a Credible Threat and Should an Internet Service Provider Be Liable If It Does?*, 17 SANTA CLARA HIGH TECH. L.J. 115, 116 (2001) (claiming the victim wrote the following message, "Tell me you have a package, and when I open my door, attack me. Tie me, gag me, rip off my clothes and go for it. I'll struggle a little just for the fun of it….").

[110] *See Myths and Facts About Stalking*, U. WIS. OSHKOSH, http://www.uwosh.edu/couns_center/campus-victim-advocate/stalking/myths-and-facts-about-stalking (last visited Apr. 18, 2017) (dispelling the myth that stalkers can or should be ignored by explaining that "[t]he fact [that] there has been no danger up until now does not mean it won't come…even if the stalker has not made [] an overtly dangerous statement, any words or behaviors that indicate an unwillingness to let go…is a red flag.").

[111] *Cassidy*, 814 F. Supp. 2d at 586.

[112] *Id.* at 586 n.14.

[113] *See generally* Gaby Dunn, *Get Rich or Die Vlogging: The Sad Economics of Internet Fame*, FUSION (Dec. 14, 2015, 7:00 AM), http://fusion.net/story/244545/famous-and-broke-on-youtube-instagram-social-media (contemplating how platforms such as YouTube and Instagram have led to the

the court's rationale in *Cassidy* potentially precludes from § 2261A(2)(A)'s protection a segment of the population that is arguably at a heightened risk of cyberstalking and harassment.

IV. EXISTENT STATE STATUTES CANNOT BE RELIED UPON TO ADDRESS THE HARMS INFLICTED BY CYBERSTALKING

In Maryland, there are three primary statutes under which the state may bring criminal charges against a person engaged in cyberstalking.[115] All three laws are inadequate and ill-suited to address the crime of stalking when it occurs through electronic mediums.

A. Maryland's Traditional Stalking and Harassment Statutes are Ill-Fitting as Applied to Cybercrimes

Maryland's dedicated stalking statute, Crim. Law § 3-802, defines stalking as "a malicious course of conduct that includes approaching or pursuing another."[116] The major issue with prosecuting a cyberstalking incident under § 3-802 is that the phrasing of the statute could be read to require a degree of physical pursuit.[117] Under this construction, cyberstalking would fall outside of the statute's purview. In *Hackley v. State*,[118] Maryland's intermediate appellate court held that physical pursuit is a necessary element of the offense. Granting certiorari, the Court of Appeals later reversed the lower court's ruling and held that the statute *includes* physical pursuit, but does not explicitly require stalkers to approach their victims.[119] Although the Court of Appeals' holding is encouraging, it remains largely inconclusive whether the entire range of activities that

popularization of web personalities and an increase in the number of individuals pursuing internet fame).

[114] *Id*.

[115] *See supra* Part IV.A.

[116] MD. CODE ANN., CRIM. LAW § 3-802(a) (LexisNexis 2012).

[117] Hackley v. State, 866 A.2d 906, 912 (Md. Ct. Spec. App. 2005) (the defendant maintained that § 3-802 required a stalker to act "in the victim's presence and with the victim's awareness.").

[118] Hackley v. State, 885 A.2d 816, 817 (Md. 2005).

[119] *Id*. ("[W]e believe that the Court of Special Appeals misconstrued the statute and shall hold that the crime of stalking does not require that the defendant approach or pursue his victim").

constitute cyberstalking would fall within the scope of § 3-802.[120] The defendant's conduct in this case conformed closely to the conventions of traditional stalking and the court heavily relied on the defendant's real world, physical actions against the victim to determine his culpability.[121] In affirming the defendant's conviction, the Court of Appeals specifically cited the fact that he physically assaulted the victim, repeatedly visited her house and left letters under the windshield wiper of her car, and approached her multiple times in the early morning.[122] *Hackley* opens the door for a possible conviction of cyberstalking under the stalking statute, but—because of the facts of the case—is a poor metric of § 3-802's viability in the cyberstalking context.

Crim. Law § 3-803, Maryland's harassment statute, is another law under which prosecutors could potentially bring criminal charges for cyberstalking. The statute, last amended in 2011, is inadequate in much the same way the stalking statute is when applied to cyberstalking.[123] Both statutes are not specifically geared towards cyberstalking and do not account for the complexities of stalking behaviors carried out online. Specifically, § 3-803 is problematic because it requires the perpetrator to receive a "reasonable warning or request to stop by or on behalf of the other."[124] This requirement poses an undue burden on victims who are either unaware of their stalker's online activities or who are otherwise unable to identify and contact their stalker because of the anonymity that the Internet confers.[125] Moreover, the statue is ambiguous as to what exactly "receipt" of a reasonable warning entails. That is, it is unclear whether a victim must prove that their stalker actually viewed the request, or whether evidence that a request was sent would suffice.

---

[120] *See* Brian Frosh & Kathleen Dumais, *Bill Targets "Rape by Proxy"*, BALT. SUN (Feb. 3, 2014), http://articles.baltimoresun.com/2014-02-03/news/bs-ed-internet-sexual-assaults-20140203_1_victim-prince-george-jilted-lover (citing a Prince George's County case where more than 50 men accosted a woman and her children at home after her ex-husband posted ad requests such as "Rape Me and My Daughters," Maryland Attorney General Brian Frosh explained that "prosecutors were forced to cobble together a lengthy list of charges to accumulate a sentence that would fit this novel crime.").

[121] Hackley, 885 A.2d at 822.

[122] *Id*.

[123] MD. CODE ANN., CRIM. LAW § 3-803 (LexisNexis 2011).

[124] *Id.* § 3-803(2).

[125] *See supra* Part II.B.

B. Maryland's Misuse of Electronic Mail Act Suffers from the Same Limitations that Render the State's Harassment Statute Ineffective

Maryland's Misuse of Electronic Mail Act, § 3-805, is perhaps the state's primary vehicle for prosecution of a cyberstalker.[126] Unlike the stalking and harassment statutes, § 3-805 explicitly prohibits the use of "electronic communication" to "maliciously engage in a course of conduct…[that] harass[es], alarm[s], or annoy[s] the other."[127] Although the state's enactment of this measure is laudable, its utility to victims of cyberstalking is critically undermined by the inclusion of § 3-803's qualification that the offender must receive "a reasonable warning or request to stop by or on behalf of the other."[128] Indeed, the term "electronic communication" is limited only to "the transmission of information, data, or a communication…*that is sent to a person* and *that is received by the person*" (emphasis added).[129] Because of this, the statute discounts a variety of behaviors such as when stalkers enlist third parties to help effectuate their goals[130] or when blogs and web sites such as Facebook and Twitter are used to make defamatory posts that are either unknown to a victim or not specifically directed at a victim.[131]

Furthermore, § 3-805 is puzzling in that "conduct that inflicts serious emotional distress" falls within its scope of prohibited behaviors only when the conduct is directed towards a minor.[132] The increased scope of prohibited computer activities under § 3-805(b)(1)(2) is apt in that minors are a vulnerable subset of the population to whom the State should afford special consideration.[133]

---

[126] MD. CODE ANN., CRIM. LAW § 3-805 (LexisNexis 2002 & Supp. 2016).
[127] *Id.* § 3-805(b)(1)(i).
[128] *Id*. § 3-805(b)(1)(ii).
[129] *Id*. § 3-805(a)(1)(2).
[130] *See* Black, *supra* note 59.
[131] *See Cassidy*, 814 F. Supp. 2d at 579 n.6 (categorizing a number of the defendant's Tweets as not necessarily directed towards the plaintiff).
[132] MD. CODE ANN., CRIM. LAW § 3-805(b)(1)(2).
[133] *See generally* Charisse L. Nixon, *Current Perspectives: The Impact of Cyberbullying on Adolescent Health*, 5 ADOLESCENT HEALTH, MED., THERAPEUTICS 143, 144 (2014) (correlating cyberbullying with the onset of depressive symptomology such as feelings of "sadness, hopelessness, and powerlessness"

However, emotional distress is no less serious or injurious when inflicted on adult victims of cyberstalking.[134] Emotional distress, impaired psychological well-being, and decline in cognitive health are some of the most well-documented harms that result from stalking.[135] The state's prohibition of "conduct that inflicts serious emotional distress"—but only as applied to minors—shows a fundamental lack of understanding as to one of the basic components of stalking.[136]

V. JUSTICE FOR MARYLAND CYBERSTALKING VICTIMS STARTS WITH ADOPTION OF A STATUTE THAT FITS THE CRIME

As of November 2016, only six states have adopted separate laws that expressly target cyberstalking.[137] Of these states, three—Illinois, Rhode Island, and Washington—have laws that address solicitation of third party participants, and are thus likely to be expansive enough to encompass the range of activities that constitute cyberstalking.[138]

---

among adolescents); *see also* Maia Szalavitz, *The Tragic Case of Amanda Todd*, TIME (Oct. 16, 2012), http://healthland.time.com/2012/10/16/the-tragic-case-of-amanda-todd (chronicling the events that led to fifteen year-old Amanda Todd's suicide after an online predator cyberstalked and blackmailed her with sexually explicit photographs that he manipulated her into providing when Todd was just twelve years old).

[134] *See* Goodno, *supra* note 4, at 128 (discussing how stalking may cause "post-traumatic stress disorder, depression and serious emotional distress" in victims).

[135] Lynne Roberts, *Jurisdictional and Definitional Concerns with Computer-Mediated Interpersonal Crimes: An Analysis on Cyber Stalking*, 2 INT'L J. CYBER CRIMINOLOGY 271, 273 (2008) (noting that "[t]he ongoing experience of vulnerability may create more psychological distress than an actual physical assault").

[136] *See* Avlana K. Eisenberg, *Criminal Infliction of Emotional Distress*, 113 MICH. L. REV. 607, 609 (2015) (distinguishing stalking, bullying, and harassment as fundamentally "criminal infliction of emotional distress" crimes; that is, crimes for which the law "imposes liability for causing another person emotional harm.").

[137] 720 ILL. COMP. STAT. 5/12–7.5 (2013); LA. STAT. ANN. § 14:40.3 (2010); MISS. CODE ANN. § 97-45-15 (West 2003 & SUPP. 2016); N.C. GEN. STAT. § 14-196.3 (West 2015); 11 R.I. GEN. LAWS § 11-52-4.2 (West 2008); WASH. REV. CODE ANN. § 9.61.260 (2004).

[138] *See* 11 R.I. GEN. LAWS § 11-52-4.2 ("Whoever transmits any communication by computer or other electronic device to any person or *causes any person to be contacted for the sole purpose of harassing that person or his or her family* is guilty" …(emphasis added)); *see also* WASH. REV. CODE ANN. § 9.61.260 ("A person is guilty of cyberstalking if he or she, with intent to harass, intimidate, torment, or embarrass any other person, and under circumstances not constituting telephone

In formulating its own cyberstalking law, Maryland should look to these states for guidance, but also be progressive in addressing the ambiguities that make prosecuting and convicting offenders at the federal[139] and state level difficult.[140] Ultimately, the success of a prospective cyberstalking statute will hinge on the State's ability to articulate clear standards of *actus reus* and *mens rea* that (1) are expansive enough to cover the range of activities that occur in cyberspace,[141] and (2) do not unfairly prejudice victims.[142]

A. An Actus Reus Standard that is Broad Enough to Account for the Variety of Behaviors that Could Constitute Cyberstalking

Engaging in a "malicious course of conduct" that puts another in "reasonable fear of serious bodily injury" is the critical *actus reus* requirement of Maryland's current stalking statute.[143] As for the *actus reus* requirement of a prospective cyberstalking statute, engagement in a "course of conduct" should also be the essential physical act needed to establish criminal liability.[144] As Naomi Goodno points out in *Cyberstalking, A New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, "punishing merely one instance of harassing conduct may unjustly penalize one who acts once out of anger, versus one who engages in a series of terrifying acts."[145] Generally, it is difficult to quantify exactly when certain actions lose their independence and become recognized as part of a "course" of behavior.[146] With respect to cyberstalking, however, "course of

harassment, makes an electronic communication to such other person *or a third party*" (emphasis added)).

[139] *See supra* Part III.

[140] *See supra* Part IV.

[141] *See infra* Part V.A.

[142] *See infra* Part V.B.

[143] Hackley, 885 A.2d at 820.

[144] *See* Shimizu, *supra* note 26, at 117. By its definition, stalking requires a course of conduct; singular incidents or occurrences do not qualify. *Id*.

[145] Goodno, *supra* note 4, at 134.

[146] RICHARD CARD, CARD, CROSS, AND JONES: CRIMINAL LAW 217 (21st ed. 2014) ("It is not simply a matter of counting the number of incidents. There must be a sufficient connection between the acts in type and context as to justify the conclusion that they amount to a *course* of conduct."). Nor can course of conduct be presupposed by looking at timeframes—sending an email or message every year on

conduct" must be taken to mean two or more occasions.[147] A more stringent definition that uses any number other than two as the baseline for establishing a pattern would only challenge offenders to inflict the greatest degree of harm in the least number of incidents possible.[148]

The *actus reus* component of a cyberstalking statute must also be expansive enough reflect the complexities of stalking crimes. A key shortcoming of Maryland's traditional stalking law is that "a malicious course of conduct" is defined only as behaviors that place another in reasonable fear of "serious bodily injury," "an assault in any degree," "rape or sexual offense," "false imprisonment," or "death."[149] Stalking, especially in the context of domestic violence, is about more than just explicit threats of violence; it is a crime of power and control.[150] The means through which offenders undermine the autonomy of their victims, and the type of harms inflicted are many and varied.[151] Consequently, Maryland's cyberstalking statute must broadly cover online conduct that inflicts not only physical injury, but also psychological and emotional distress—conduct that threatens not just the safety of victims, but also the safety of loved ones.[152]

---

a particular date and calling three separate times in rapid succession are examples of behaviors that take place on drastically different time lines, but may nevertheless both amount to a course of conduct. *Id.*

[147] The federal stalking statute and some states use two as the minimum number of incidents required to establish a course of conduct. 18 U.S.C. § 2266 (2012) ("The term 'course of conduct' means a pattern of conduct composed of 2 or more acts, evidencing a continuity of purpose."); *see also* D.C. CODE § 22-3132 (2009) ("'To engage in a course of conduct' means directly or indirectly, or through one or more third persons, in person or by any means, on 2 or more occasions".).

[148] *See* discussion *infra* Part V.B. Just as setting two as the baseline in traditional stalking statutes does not cast an overly broad net, it is a similarly appropriate minimum as applied to cyberstalking statutes. Those who innocuously or accidently perform an act that constitutes cyberstalking more than once will remain shielded due to absence of *mens rea*.

[149] MD. CODE ANN., CRIM. LAW § 3–802(a)(1).

[150] *See* Major, *supra* note 44 and accompanying text.

[151] Roberts, *supra* note 135, at 273.

[152] *See* KATRINA BAUM ET AL., STALKING VICTIMIZATION IN THE UNITED STATES 2, OFFICE OF JUST. PROGRAMS, U.S. DEP'T JUST. (2009) ("The fears and emotional distress that stalking engenders are many and varied…. About 4 in 10 stalkers threatened the victim or the victim's family, friends, co-workers, or family pet.").

Finally, regarding Maryland's harassment statute, the requirement that a person must receive "a reasonable warning or request to stop," before the conduct becomes criminal is impractical as applied to cyber-based crimes.[153] As discussed, in many cases, victims are not aware of their stalker's online activities, or if they are aware, they may not be able to identify their stalkers sufficiently to issue a warning.[154]

B. A Standard of Mens Rea that Allows for Proper Identification of "Credible Threats" in Cyberspace

The *mens rea* element of cyberstalking should be an objective standard that looks to whether a reasonable person "would take the statement as a serious expression of an intention to inflict bodily harm."[155] The alternative, a subjective standard that instead looks to whether a reasonable person "would foresee that the listener would interpret the speech as a threat of violence" places too arduous a burden on the government and victim.[156] Under the subjective standard, a defendant who places a victim in reasonable fear of serious bodily injury or death will go unpunished if the government cannot prove, beyond a reasonable doubt, that the defendant understood the communication to be threatening.[157] Under ordinary circumstances, this burden of proof is exceedingly difficult to satisfy.[158] In the context of electronic communications, it would be nearly impossible because cues such as tone of voice, facial expression, and demeanor are unavailable in cyberspace. Consequently, defendants could always allege that a comment was made in jest or simply misinterpreted by the victim.[159]

---

[153] MD. CODE ANN., CRIM. LAW § 3-803(a)(2).
[154] *See supra* notes 53–54, 63–68 and accompanying text.
[155] *Alkhabaz*, 104 F.3d at 1494 (internal citation omitted).
[156] McCann, *supra* note 79, at 528.
[157] Vikram D. Amar & Alan E. Brownstein, *The Supreme Court to Consider When Threats Can Be Punished Consistent with the First Amendment*, JUSTIA (Oct. 10, 2014), https://verdict.justia.com/2014/10/10/supreme-court-consider-threats-can-punished-consistent-first-amendment.
[158] *See* Jackson v. Virginia, 443 U.S. 307, 315 (1979) (defining "beyond reasonable doubt" as "a subjective state of near certitude of the guilt of the accused").
[159] *See* NANCY WILLARD, EDUCATOR'S GUIDE TO CYBERBULLYING AND CYBERTHREATS 3, CTR. SAFE & RESPONSIBLE USE OF THE INTERNET (2007), https://education.ohio.gov/getattachment/Topics/Other-Resources/School-Safety/Safe-and-Supportive-Learning/Anti-Harassment-Intimidation-and-Bullying-

An objective determination of whether or not an individual intended to inflict harm is the appropriate standard because "like an offline stalker, a cyberstalker should have to 'intentionally' engage in conduct that causes his target to fear for her safety" in order to be held criminally liable.[160] However, it is also important to consider that, in many cases of cyberstalking, the victim knows the offender and is likely to have had some sort of relationship with him.[161] In the context of cyberstalking as part of domestic violence, the objective standard should be flexible enough to acknowledge that not all threats are blatantly obvious.[162] Comments and actions of the offender must be situated in the context of the relationship between the offender and victim.[163] An assessment of this nature that looks to the totality of the circumstances is consistent with an objective standard of *mens rea*.[164] Similar to how courts assess an officer's determination of probable cause,[165] a court should consider whether a reasonable person *in the*

Resource/Educator-s-Guide-Cyber-Safety.pdf.aspx (discussing the difficulty and ambiguity of interpreting communications in cyberspace).

[160] Goodno, *supra* note 4, at 134. Inclusion of this intent requirement is crucial—in 2016, the Illinois Appellate Court held that both Illinois' general stalking and cyberstalking statutes were "facially unconstitutional under the due process clause of the fourteenth amendment," for lack of a *mens rea* standard, *i.e*., that a person must actually intend to inflict emotional distress. People v. Relerford, 56 N.E.3d 489, 495–97 (Ill. App. Ct. 2016). As of April 7, 2017, the case is still pending after the Illinois Supreme Court granted the State's appeal as a matter of right. DAVID BERGSCHNEIDER, SUMMARY OF SIGNIFICANT CRIMINAL ISSUES PENDING IN THE ILLINOIS SUPREME COURT 3, OFFICE OF THE STATE APPELLATE DEFENDER (2017), https://www.illinois.gov/osad/Publications/Documents/pend.pdf.

[161] *See* Fisher & Sloan, *supra* note **Error! Bookmark not defined.** ("When specifically examining perpetrators who are known to the victim, the most common victim/offender relationships were friends/former friends (25.4%), boyfriends/ex-boyfriends (12.1%) . . .").

[162] *See* Major, *supra* note 44 and accompanying text.

[163] *See supra* notes 19–31 and accompanying text.

[164] *Alkhabaz*, 104 F.3d at 1494 (internal citation omitted).

[165] *See* Illinois v. Gates, 462 U.S. 213, 231 (1983) (noting that an officer's determination of probable cause "must be seen and weighed not in terms of library analysis by scholars, but as understood by those versed in the field of law enforcement."); *see also* Susan F. Mandiberg, *Reasonable Officers vs. Reasonable Lay Persons in the Supreme Court's* Miranda *and Fourth Amendment Cases*, 14 LEWIS & CLARK L. REV. 1481, 1496 (2010) ("Although the issuing magistrate is the one who must draw conclusions, the perspective of the reasonable officer is central to the inquiry.").

victim's place "would take the statement as a serious expression of an intention to inflict bodily harm."[166]

C. A Proposed Amendment to Maryland's Criminal Code

This Comment proposes an amendment of Maryland's criminal statutes to incorporate the following cyberstalking legislation. Borrowing judiciously and generously from the language of Illinois and Washington's cyberstalking statutes,[167] the proposal is broad enough to sufficiently address the multifaceted nature of cyberstalking. The prescribed *mens rea* and *actus reus* requirements are formulated to minimize any chilling effect on First Amendment protections:

> A person shall be found guilty of the crime of cyberstalking if:
>
> (a) He or she—with the intent to harass, intimidate, coerce, threaten, embarrass, or torment—uses a form of electronic communication on at least two separate occasions in a manner that would cause a reasonable person to:
>
> (1) Fear for his or her own safety, or the safety of another person, or
>
> (2) Suffer serious psychological or emotional distress.
>
> When committed as part of a course of conduct, proscribed activities include, but are not limited to:
>
> (a) The use of any lewd, lascivious, indecent, or obscene words, images, or language, or suggesting the commission of any lewd or lascivious act;[168]
>
> (b) Threats of assault, sexual or otherwise, directed at a person's self, their property, or any member of their family or household

[166] *Alkhabaz*, 104 F.3d at 1494 (citation omitted).
[167] 720 ILL. COMP. STAT. 5/12-7.5, *invalidated by* People v. Relerford, 56 N.E.3d 489 (Ill. App. Ct. 2016); WASH. REV. CODE ANN. § 9.61.260.
[168] WASH. REV. CODE ANN. § 9.61.260(1)(a).

(c) Solicitation of third parties to commit an act in violation of any provision of this code

For the purposes of this Section:

"Course of conduct" shall be taken to mean a pattern of conduct composed of two or more acts that is without legitimate reason and evidences a unity of purpose.

"Electronic communication" shall be taken to mean the transmission of information by wire, radio, optical cable, electromagnetic technology, or any other similar means. This includes, but is not limited to, e-mail, social media platforms, websites, pager service, text messaging, voice mail, and other internet-based channels of communication.[169]

"Reasonable person" shall be taken to mean a person in the victim's circumstances, with the victim's knowledge of the defendant, with the victim's knowledge of the defendant's prior acts, and within the context of the victim's relationship with the defendant.

"Third parties" shall be taken to mean any person other than the person violating these provisions and the victim or persons towards whom the violator's actions are directed.[170] A person who solicits a third party to violate the provisions of this Section will be found guilty of cyberstalking just as surely as if the person committed the act him or herself.

CONCLUSION

California passed the first stalking statute in 1990.[171] By 1993, almost all 50 states and the District of Columbia had amended their

[169] Adapted from WASH. REV. CODE ANN. § 9.61.260(5).

[170] Adapted from 720 ILL. COMP. STAT. 5/12–7.5(C)(7), *invalidated by* People v. Relerford, 56 N.E. 3d (Ill. App. Ct. 2016).

[171] Christine B. Gregson, Comment, *California's Antistalking Statute: The Pivotal Role of Intent*, 28 GOLDEN GATE U.L. REV. 221 n.2 (1998) (enacting the nation's first anti-stalking statute, California was the first state to criminalize the repeated

penal codes with some form of anti-stalking legislation.[172] This process through which society recognizes and responds to deviant behaviors through legislative reform is fundamental to the preservation of law and order. The reality that we must confront is that technological innovation has drastically expanded the scope of stalking victimizations.[173] Without parallel development in laws, stalkers who utilize electronic mediums to achieve their ends will continue to fall through gaps in federal and state statutory schemes.[174] Instead of amending traditional stalking laws in ways that ultimately prove to only be half measures,[175] separate and distinct cyberstalking statutes are needed that can be properly scoped to reflect the realities of modern society.

following or harassment of another person "with the intent to place that person in reasonable fear for his or her safety, or the safety of his or her immediate family").

[172] Shonah Jefferson & Richard Shafritz, *A Survey of Cyberstalking Legislation*, 32 U. WEST. L.A. L. REV. 323, 326–27 (2001).

[173] *See supra* Part II.B.

[174] *See supra* Part III–IV.

[175] *See* discussion *supra* Part III.B.