2015

Communication in Cyberspace

Nancy Leong

Joanne Morando

Recommended Citation
94 North Carolina Law Review, 2015, Forthcoming

Communication in Cyberspace

COMMUNICATION IN CYBERSPACE

Nancy Leong[*] *& Joanne Morando*[+]

ABSTRACT

This Article examines a problem in cybercrime law that is both persistent and pervasive. What counts as "communication" on the Internet? Defining the term is particularly important for crimes such as cyberstalking, cyberharassment, and cyberbullying, where most statutes require a showing that the alleged perpetrator "communicated" with the victim or impose a similar requirement through slightly different language.

This Article takes up the important task of defining communication. As a foundation to our discussion, we provide the first comprehensive survey of state statutes and case law relating to cyberstalking, cyberharassment, and cyberbullying. We then examine the realities of the way people use the Internet to develop a definition of "communication" that reflects those realities. That is, we aim to provide effective tools by which prosecutors can address wrongful conduct without punishing innocuous behavior or chilling speech. We conclude by proposing a model statute that appropriately defines "communication." We recommend that state legislatures adopt the statute or modify existing laws to match it in pertinent part and demonstrate how the statute would apply in a range of situations.

[*] Associate Professor, University of Denver Sturm College of Law.

[+] J.D. expected, May 2015, University of Denver Sturm College of Law.

THIS PAPER IS UNDERGOING EDITING AND REVISIONS. DO NOT QUOTE OR CITE WITHOUT THE EXPRESS WRITTEN PERMISSION OF BOTH AUTHORS.

TABLE OF CONTENTS

THIS PAPER IS UNDERGOING EDITING AND REVISIONS. DO NOT QUOTE OR CITE WITHOUT THE EXPRESS WRITTEN PERMISSION OF BOTH AUTHORS.

INTRODUCTION

"Elizabeth Long needs to stop bitching about how she almost killed herself and go ahead and do it."[1] This message was posted anonymously and broadcast over a 1.5-mile radius, reaching thousands of individuals who had downloaded an app called Yik Yak.[2] During a series of events that would become known as GamerGate, Zoe Quinn was forced to leave her home, fearing for her safety, after her address was posted online.[3] This act of revealing personal information and documents to the public online is called "doxxing," and it has become increasingly common in recent years.[4] Brianna Wu, who owns a video game company, woke up to the following message posted to Twitter: "Guess what bitch? I now know where you live. You and Frank [her husband] live at [REDACTED]."[5] A fake Twitter account titled "Anita Needs to Die" features a profile picture of Anita Sarkeesian, a feminist commentator, with photoshopped black eyes and a bloody nose.[6]

In the past, statutes criminalizing behavior such as threats, stalking, and harassment generally require that the speaker

---

[1] Alyson Shontell, *How Two Georgia Fraternity Brothers Created Yik Yak, a Controversial App That Became a ~$400 Million Business in 365 Days*, BUSINESS INSIDER (Mar. 13, 2015), http://www.businessinsider.com.au/the-inside-story-of-yik-yak-2015-3.

[2] *Id.*

[3] Alex Hern, *Zoe Quinn on Gamergate: 'We Need a Proper Discussion About Online Hate Mobs,'* THE GUARDIAN (Sept. 12, 2014), http://www.theguardian.com/technology/2014/sep/12/zoe-quinn-gamergate-online-hate-mobs-depression-quest.

[4] *Id.*

[5] Ian Miles Cheong, *Game Developer Brianna Wu Driven From Home After Death Threats and Doxxing*, GAMERANX (Oct. 10, 2014), http://www.gameranx.com/updates/id/24642/article/game-developer-brianna-wu-driven-from-home-after-death-threats-and-doxxing/. In almost all republications and screenshots of doxxing occurrences, the information at issue has been removed or redacted to avoid further dispersing the private information.

[6] Since deleted, a screen capture can be found at Carly Smith, *GamerGate: A War on Women Hiding Behind a Mask of "Ethics,"* INDIEWIRE (Oct. 17, 2014), http://blogs.indiewire.com/womenandhollywood/gamergate-a-war-on-women-hiding-behind-a-mask-of-ethics-20141017.

"communicate" with the target. It is easy to establish that communication took place when the behavior takes the form of a phone call or letter directly to the target. But the Internet, along with various social media platforms and apps, have enabled other forms of directing abuse at targets in which "communication" cannot be defined simply as direct messages from one person to another. Understanding the ways people communicate on the Internet is vitally important to creating laws that regulate harmful online speech and conduct.

In this Article, we present an original empirical survey and analysis of three types of such laws in the federal code and all fifty states: cyberstalking laws, which prohibit a pattern of online behavior that poses a credible threat of harm;[7] cyberharassment laws, which prohibit online activity that torments or distresses its target;[8] and cyberbullying laws, which generally refer to harassment and bullying among minors.[9] These three categories of laws are related and often overlap, so the distinction among them is not always clear. More importantly, however, all three are intended to address essentially the same problem: the use of the Internet to engage in speech and behavior that seriously damage people's lives.

When we consider the behavior that these laws are designed to prevent, the need to define communication becomes clear. For example, a law designed to prohibit cyberharassment

---

[7] *See Cyberstalking and Cyberharassment Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 12, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx

[8] *See id.*

[9] *See id.* We did not engage in a census of state cyberbullying laws for purposes of this project, although other commentators have systematically examined such laws. *See, e.g.*, Jacqueline D. Lipton, *Combating Cyber-Victimization*, 26 BERKELEY TECH. L.J. 1103, 1122 (2011); Alison Virginia King, Note, *Constitutionality of Cyberbullying Laws: Keeping the Online Playground Safe for Both Teens and Free Speech*, 63 VAND. L. REV. 845, 857–64 (2010). Our conclusions about what should count as communication for purposes of cyberstalking and cyberharassment statutes would, however, apply equally well to cyberbullying statutes, perhaps with the addition of forums unique to minors (for example, an intranet message board available exclusively to students at a particular school).

would be essentially useless if its scope was limited to emails. A harasser has many other ways of communicating with a target, such as Facebook posts and messages, Tweets, blog posts, and blog comments. At the same time, a law designed to prohibit cyberharassment would be decidedly overbroad—and would violate the First Amendment—if it prohibited *all* negative speech about an individual on the Internet.

Our project, then, is to develop a definition of communication that will allow for the punishment of harmful speech without sweeping in innocuous speech or running afoul of the First Amendment. There are, of course, other issues necessary to resolve to draft cyberharassment and cyberstalking statutes—for example, the mental state necessary for criminalization, the frequency and severity of harmful speech, and the effect of such speech on the victim. But defining what "communication" means in the online world is uniquely critical for cyberharassment statutes, as the other elements are, for the most part, well defined by other areas of criminal law that use the same or similar standards.

We conclude that "communication" on the Internet should be defined as any online behavior—including, but not limited to, speech—by an individual that the individual either knew the target would discover or recklessly disregarded a reasonable likelihood that the target would discover. We select the standard for a number of reasons. First, we think it appropriate to hold individuals liable for behavior that they know or are reckless in ignoring that the target of the behavior would discover. The use of a recklessness standard with respect to an individual's mental state strikes a balance between a standard requiring actual knowledge—which would in many instances be very difficult for the prosecution to prove—and mere negligence—which risks criminalizing accidental behavior. By defining a communication as behavior performed with reckless disregard for the likelihood that the target will find out about it, we sweep in behavior that an individual knew the target of the behavior would discover, as well as behavior that an individual consciously disregarded the likelihood that the target would discover.

Moreover, this approach is consonant with the Supreme Court's questioning during oral argument for *Elonis v. United*

States,[10] which was argued in December and in which the Supreme Court's decision is currently pending.[11] *Elonis* involved a man who made violent statements about his ex-wife on Facebook.[12] The statements would have caused a reasonable person to fear for her safety, and Elonis was convicted under the federal threats statute.[13] The issue in *Elonis*, then, is whether the government must prove that the perpetrator *intended* to threaten the target, or whether it is enough to show that a reasonable target would have felt threatened and that this target in fact felt threatened. At oral argument, the Justices seemed skeptical that the prosecution would have to prove intent to threaten, with Justice Alito noting that to do so "sounds like a roadmap for threatening a spouse and getting away with it."[14] Justice Kagan instead suggested a recklessness standard, which would be easier for the prosecution to prove.[15]

Elonis does not directly implicate our purpose in this Article. Rather, it speaks to whether a perpetrator intends statements to threaten, while our concern is with whether a perpetrator intends or ignores the likelihood that statements will be seen by the subject. We think, however—and will explain in more detail in the body of the Article—that a consistent recklessness standard creates an appropriate parallel between the intent requirement associated with the intent to threaten or engage in other harmful speech and the intent requirement associated with the communication itself.[16]

---

[10] 730 F.3d 321 (3d Cir. 2013), *cert. granted*, 134 S. Ct. 2819 (2014).

[11] *See, e.g.*, Lyle Denniston, *Argument Analysis: Taking Ownership of an Internet Rant*, SCOTUSBLOG (Dec. 1, 2014), http://www.scotusblog.com/2014/12/argument-analysis-taking-ownership-of-an-internet-rant/ (recapping oral argument of *Elonis* before the Supreme Court).

[12] *Elonis* 730 F.3d at 323.

[13] 18 U.S.C. § 875 (2012); *Elonis*, 730 F.3d at 323.

[14] Transcript of Oral Argument at 59 lines 20–22, Elonis v. United States (2014), *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/13-983_4f57.pdf.

[15] *Id.* at 8 lines 16–21.

[16] To the extent that the *Elonis* decision does overlap with our current prescription, we may revise the Article slightly. Such overlap is highly unlikely given that an entirely different element of the crime is at issue, but even dicta

Finally, a note about terminology: While our survey of state laws and cases examines the way that communication is defined for cyberharassment and cyberstalking statutes, we will use the term "cyberharassment" to refer collectively to both of these types of statutes. When we are referring only to cyberharassment statutes, and not to cyberstalking statutes, we will make that clear in individual instances. In some cases, our analysis will also apply to cyberbullying statutes, given that those statutes also deal with what constitutes electronic communication, although we did not specifically examine those statutes in our empirical survey. We note where our discussion extends to cyberbullying statutes as well.

The Article proceeds as follows. In Part I, we discuss the importance of defining "communication" on the Internet. We survey the relevant scholarly literature on electronic communication, noting that no previous work has examined in detail what it means to communicate on the Internet in light of the myriad ways of doing so. We then examine the realities of how people use the Internet to convey information to one another and explain what it should mean to "communicate" online in light of these realities.

In Part II, the Article undertakes an original empirical survey of statutes criminalizing cyberharassment, taking stock of the way that "communication" is currently statutorily defined and judicially interpreted. We first survey the way communication is defined in state statutes relating to cyberharassment and develop a typology of such statutes. We then examine the way that state courts have interpreted the meaning of communication according to these statutes.

Finally, Part III develops an agenda for implementing a better definition of communication. We point out the defects in existing laws, describe how they can be ameliorated, and propose statutory language that legislators should use in passing new cyberharassment statutes or amending old ones. Ultimately, these proposals will yield cyberharassment laws that accurately reflect the way that people use the Internet.

---

from the Supreme Court may provide an interesting addition to our analysis here.

I. WHAT QUALIFIES AS COMMUNICATION?

This Part considers what should count as "communication" on the Internet. It surveys the existing scholarly literature, which has not examined this issue in great detail. It then examines the way that people use the Internet, taking account of existing technology in a way that neither scholars nor judges have thus far. Ultimately, we adopt a practical definition of "communication" based in the way people actually transmit and receive information via the Internet.

A. A Neglected Element of Cyberharassment

The evolution of cyberharassment law has presented many novel issues for legal debate, including questions of constitutionality,[17] burdens of proof,[18] and the feasibility of

[17] Considerable scholarship focuses on what is necessary to make such cyberharassment statutes compliant with the requirements of the First Amendment. *See, e.g.*, Andrew B. Carrabis & Seth D. Haimovitch, *Cyberbullying: Adaptation from the Old School Sandlot to the 21st Century World Wide Web—The Court System and Technology Law's Race to Keep Pace*, 16 J. TECH. L. & POL'Y 143 (2011) (analyzing First Amendment concerns of Florida's cyberbullying laws in contrast to the seminal cases of free speech in public schools); Lyrissa Lidsky & Andrea Pinzon Garcia, *How Not to Criminalize Cyberbullying*, 77 MO. L. REV. 693 (2012) (presenting "a First Amendment primer to guide law-makers); Ari Ezra Waldman, *Hostile Educational Environments*, 71 MD. L. REV. 705 (2012) (discussing the interaction of the First Amendment and a school's ability to punish off-campus cyberbullying); Alison Virginia King, Note, *Constitutionality of Cyberbullying Laws: Keeping the Online Playground Safe for Both Teens and Free Speech*, 63 VAND. L. REV. 845 (2010) (offering "suggestions for how cyberbullying laws can be crafted to address the problem of online bullying while not eroding First Amendment Freedoms").

[18] *See, e.g.*, David Gray, Danielle Keats Citron & Liz Clark Rinehart, *Fighting Cybercrime After* United States v. Jones, 103 J. CRIM. L. & CRIMINOLOGY 745 (discussing Fourth Amendment implications in securing evidence of cybercrime); Aimee Fukuchi, Note, *A Balance of Convenience: The Use of Burden-Shifting Devices in Criminal Cyberharassment Law*, 52 B.C. L. REV. 289 (2011) (proposing burden-shifting devices because the prosecution is procedurally disadvantaged in proving the details of the crime that are "peculiarly within the knowledge of the accused"); Kori Clanton, *We Are Not*

implementation.[19] While each of these considerations is essential to the formation of the law, we must still ask a foundational question: what specific conduct is the legislature trying to criminalize? The answer to that question lies in how we define communication, or, put differently, what it means to communicate online.

Policy makers and scholars have considered two different approaches to defining communication. The first is target-centric—it examines how the target of the communication is affected or reached by that communication. The second is speaker-centric—it examines the means or platform that the speaker uses to communicate. Yet a clear definition of communication requires both understandings.

In a target-centric discussion of cyberharassment, the focus is on the wide variety of ways that harassers can harm their targets.[20] Targets can be directly harassed or threatened by one

---

Who We Pretend to Be: ODR Alternatives to Online Impersonation Statutes, 16 CARDOZO J. CONFLICT RESOL. 323, 340–41 (2014) (noting the difficulty in the plaintiff or victim having the burden of identifying a perpetrator that operated in anonymity).

[19] We note, moreover, that while many student authors have made interesting and relevant contributions relating to feasibility of implementation, the issue is lacking in commentary by established academics and practitioners. *See, e.g.*, Cassie Cox, *Protecting Victims of Cyberstalking, Cyberharassment, and Online Impersonation Through Prosecutions and Effective Laws*, 54 JURIMETRICS J. 277 (2014) (noting the difficulties in proving the required culpable mental state); Heather Benzmiller, Note, *The Cyber-Samaritans: Exploring Liability for the "Innocent" Bystanders of Cyberbullying*, 107 NW. U. L. REV. 927 (2013) (discussing the need to criminalize the role of the bystander that escalates the cyberbullying); Arthur Gaus, Comment, *Trolling Attacks and the Need for New Approaches to Privacy Torts*, 47 U.S.F. L. REV. 353 (2012) (proposes that a tort regime be the primary way to deal with cyberharassment as the internet anonymity makes traditional criminal culpability difficult); Kate E. Schwartz, Note, *Criminal Liability for Internet Culprits: The Need for Updated State Laws Covering the Full Spectrum of Cyber Victimization*, 87 WASH U. L. REV. 407 (2009) (noting the myriad types of cyber victimization and proposing a legislative scheme that anchors liability to the culprit's intent and the harm the victim suffered).

[20] *See, e.g.*, DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 29 (2014) (discussing cyberharassment's ability to affect the "victims' professional reputations and careers, discourage[e] on- and offline pursuits, disrupt[] both crucial and ordinary life choices, and cause[] physical and emotional harm"); Cassie Cox, *Protecting Victims of Cyberstalking, Cyberharassment, and Online*

person.[21] Or the harassment can be indirect.[22] Jacqueline Lipton notes that "cyberbullying comes in a variety of different forms, not all of which involve direct communications with the victim. . . . [O]ne key difference between victimizing an individual in the real world and online is that the victim is not always the direct recipient of the threatening or harassing communications."[23] A cyberharasser can recruit friends or other online networks to target their attack,[24] assuming that the content of the interaction will find its way to the intended target.[25] The target's personal information can be revealed online.[26] A cyberharasser could post false

---

Impersonation Through Prosecutions and Effective Laws, 54 JURIMETRICS J. 277, 277 (2014) (noting that "cyberstalkers can use a wider range of methods, from tracking victims through social media to impersonating targeted individuals").

[21] Direct harassment was at issue in the *Elonis* case. United States v. Elonis, 730 F.3d 321 (3d Cir. 2013). Elonis posted violent statements about his ex-wife, including "I'm not going to rest until your body is a mess, soaked in blood and dying from all the little cuts." *Id.* at 325.

[22] Indirect cyberharassment has very little in common with real world harassing activities. *See* Lipton, *supra* note 9, at 1112.

[23] Jacqueline D. Lipton, *Cyberbullying and the First Amendment*, 14 FLA. COSTAL L. REV. 99, 105 (2012).

[24] For a discussion of the unique ways the internet encourages harmful group-think see Scott Hammack, *The Internet Loophole: Why Threatening Speech On-Line Requires a Modification of the Courts' Approach to True Threats and Incitement*, 36 COLUM. J.L. & SOC. PROBS. 65, 82 (2002).

[25] One reporter described this as "crowd-sourced revenge" when her number was posted on Craigslist in the personals section, leading to hours of people calling her. Kashmir Hill, *What Are the Legal Penalties For Using Craigslist To Crowd-Source Revenge?*, FORBES (Sept. 08, 2014), http://www.forbes.com/sites/kashmirhill/2011/09/08/what-are-the-legal-penalties-for-using-craigslist-to-crowd-source-revenge/. Most infamous was the case of an ex-boyfriend posting to Craigslist under the guise of his ex-girlfriend seeking to play out a rape fantasy. Kashmir Hill, *A Reason Not to Respond to Rape Fantasy Ads on Craigslist*, ABOVE THE LAW (Feb. 16, 2010), http://abovethelaw.com/2010/02/a-reason-not-to-respond-to-rape-fantasy-ads-on-craigslist/. Tragically, the ad asked for and attracted "real aggressive man with no concern for women" who raped the woman. *Id.*

[26] This phenomenon, known as doxxing, became the focus of cyberharassment debate following GamerGate in 2014. "[D]oxxing[] involves scouring the Internet for personal data (or documents, the source of the word "doxx")—like a person's name, address, occupation, Twitter or Facebook profile—and then publicly [posting] that information." Emily Bazelon, *The*

information under the target's name.[27] Some of this conduct is online behavior that leads to offline harassment.[28]

The most common approach to defining online communication involves an examination of the means or platform that the speaker is using to engage in speech or other online behavior. For example, one scholar defines cyberharassment as speech channeled through "emails, blogs, instant messenger messages, text or video messages, chat rooms, on-line social networks, or other websites."[29] Yet even this definition from three years ago is outdated as it does not include app-based technology. As technology has evolved it is clear that cyberstalking cannot be limited to email or other "one-on-one private forums" as it once

---

Online Avengers, N.Y. TIMES MAG. (Jan. 15, 2014), http://www.nytimes.com/2014/01/19/magazine/the-online-avengers.html?_r=0. In the 2014 GamerGate controversy, many outspoken female gamers, developers, and activists were doxxed as retaliation for their public stances on GamerGate. *See* Alex Hern, *Felicia Day's Public Details Put Online After She Described Gamergate Fears*, GUARDIAN (Oct. 23, 2014), http://www.theguardian.com/technology/2014/oct/23/felicia-days-public-details-online-gamergate (minutes after Felicia Day posted about Gamergate, her address and personal email was posted in the comments section to her original post). Though not relevant to our discussion here, there has been some interesting debate over the social utility for doxxing, as a way to publicly shame poor behavior (or at least what the online community views as poor behavior). *See* Emily Bazelon, *The Online Avengers*, N.Y. TIMES MAG. (Jan. 15, 2014), http://www.nytimes.com/2014/01/19/magazine/the-online-avengers.html.

[27] Some victims reach the point that they have to include a disclaimer on their resume, explaining the negative results the employer will find should they Google their name. *See* Danielle Keats Citron, *How Cyber Mobs and Trolls Have Ruined the Internet—And Destroyed Lives*, NEWSWEEK (Sept. 19, 2014), http://www.newsweek.com/internet-and-golden-age-bully-271800 (describing Anna Mayer's issues with cyberharassment, which got to the point that "75 percent of the links appearing on the first page of a search of her name were the attack sites and disparaging posts").

[28] *See* Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61 (2007) (describing various methods of cyberharassment); Mary Anne Franks, *Sexual Harassment 2.0*, 71 MD. L. REV. 655 (2012) (noting the many ways that cyberharassers can reach their targets); Catherine E. Smith, *Intentional Infliction of Emotional Distress: An Old Arrow Targets the New Head of the Hate Hydra*, 80 DENV. U. L. REV. 1 (2002).

[29] Bradford W. Reyns et al., *Stalking in the Twilight Zone: Extent of Cyberstalking Victimization and Offending Among College Students*, 33 DEVIANT BEHAV. 1, 1, (2012).

was.[30] The original laws concerning cyberstalking and cyberharassment usually drew parallels to offline conduct criminalized under stalking and harassment laws, and in some instances drew the exact language from those statutes.

It is important to define communication as it relates to cyberactivity to prevent the all-too-easy comparison to real world criminalized activities. Lipton notes the difficulty in analogizing some types of online communication to offline analogs. For example, one might argue that gathering on a social networking site such as Facebook to make fun of a cyberbullying victim is analogous to gossiping about the victim out of her earshot.[31] Yet Lipton explains that the analogy is imperfect: "online conduct has the potential to be cut-and-pasted all over the Internet, so it is much more likely that a victim could ultimately access a transcript even when that person is not the intended recipient of the communications."[32] Likewise, the harm of online bullying is in some ways greater: "One feature of online communications is their tendency to become permanent viral records of comments about an individual."[33] As Amy Harmon observes, the myriad forms of communication available on the Internet enable cyberbullies "to be both less obvious to adults and more publicly humiliating, as gossip, put-downs, and embarrassing pictures are circulated among a wide audience of peers with a few clicks."[34]

As technology changes and becomes more pervasive, the effects of cyberharassment will too, and the law should grow to include these new forms of harassment. Laws must not be so narrowly constructed as to accidently exclude any potentially harassing conduct. Indeed, the possibilities for communication—

---

[30] Joanna Lee Mishler, *Cyberstalking: Can Communication Via the Internet Constitute a Credible Threat, and Should an Internet Service Provider Be Liable If It Does?*, Comment, 17 SANTA CLARA COMPUTER & HIGH TECH. L.J. 115 (2000) (noting that cyberstalking can take place "in public forums, rather than personal email" and that traditional anti-stalking laws should therefore "be modified to accommodate activity on the Internet").

[31] Lipton, *supra* note 23, at 108.

[32] *Id.*

[33] *Id.* at 109.

[34] Amy Harmon, *Internet Gives Teenage Bullies Weapons to Wound from Afar*, N.Y. TIMES, Aug. 26, 2004, at A1.

and thus the possibilities for cyberharassment—via the Internet are so numerous that it is virtually impossible to name them all, and new apps are emerging every day.

Attempts to list the ways in which cyberharassment could be conducted is not limited to the legal academy. The legislature and groups that promote particular public policies often adopt similar approaches. The National Conference of State Legislatures offers one such definition: "Cyberharassment usually pertains to threatening or harassing email messages, instant messages, or blog entries or websites dedicated solely to tormenting an individual."[35] A similar attempt to achieve clarity through specificity also emerges in the statutes that we examined in Part II.B.2.[36] The statutes are either silent as to what communication means or else attempt to make an inclusive list of the types of communication are included.

What is missing from the literature is a focused examination of what we mean when we discuss "communication" on the Internet. While not every cyberharassment statute in existence uses the word communication, those that do not generally impose a similar requirement using slightly different language, and the concept of communication is integral to determining what conduct we find worthy of criminalization. For example, someone who writes a lengthy series of disparaging and violent comments about another person online, but does so in a forum where the other person is virtually certain never to see it—say, in a private google document shared with no one else—no information has been transmitted to the subject of the speech, and we doubt that many people would view the speech in question as worthy of criminalization.

---

[35] *State Cyberstalking and Cyberharassment Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 12, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx. Despite having been updated 2 months prior to the writing of this Article, this definition is notably lacking considerations of apps. For example, the example in the introduction, where Elizabeth Long was told, "to stop bitching about how she almost killed herself and go ahead and do it," would not be covered under this definition as those were posts on a community forum in an app.

[36] *See infra*.

By focusing on communication, we capture what is wrong with cyberharassment, cyberstalking, and cyberbullying—that the target finds out about the speech and subsequently experiences fear, disruption, and emotional distress. These are the harms against which statutes that criminalize threats and other speech are designed to protect.[37] As Justice O'Connor explained in *Virginia v. Black*:

> The speaker need not actually intend to carry out the threat. Rather, a prohibition on true threats "protect[s] individuals from the fear of violence" and "from the disruption that fear engenders," in addition to protecting people "from the possibility that the threatened violence will occur."[38]

Understanding the ways that people communicate on the Internet, and importing that understanding into our cyberharassment statutes, is critical to addressing the harms caused by cyberharassment.

B. Internet Interaction

This section develops a typology of the myriad of ways that people communicate online and explains which categories should count as "communication." We divide online communication into five categories based on whether and how the target of the communication would know of the existence of a particular instance of Internet behavior.[39] While our specific contemporary examples—Facebook, Twitter, and so forth—will eventually become outdated as technology changes, the categories themselves are designed to be sufficiently flexible to evolve with the ways people communicate over time.

---

[37] Virginia v. Black, 538 U.S. 459–60 (2003).

[38] *Id.*

[39] We use the word "behavior" so as to encompass both speech and other forms of online activity. For example, hacking into someone's Facebook account could likely count as means of communicating with that person, but the word speech is somewhat inapt.

Today, people interact online in myriad ways. Technology allows people to engage in a wide variety of activities that include simultaneously sharing information with many friends, acquaintances, or other contacts; engaging with websites by making comments or posting original content; instant messaging; and professional and social networking. Various apps allow specialized types of communication—for example, some allow people to track their friends' location,[40] while others provide an anonymous forum for communication related to a particular institution of higher education.[41] People communicate on the Internet to perform their work functions, complete their school assignments, keep in touch with family, meet potential romantic partners, socialize with new and existing acquaintances, and virtually every other purpose of human interaction. At the touch of a button, the Internet enables us to get in touch with almost anyone, anywhere on the planet, almost instantaneously.

Social networking is an increasingly popular subset of online interaction. Many social networking apps reach over 1 million users in less than six months from their launch dates.[42] Some of the top social media websites have over 200,000,000 users, including Facebook, Twitter, and LinkedIn, and Instagram.[43] According to Facebook's website, "people use Facebook to stay connected with friends and family, to discover what's going on in

[40] *Apps – Find My Friends*, APPLE, https://www.apple.com/apps/find-my-friends/ (last visited Mar. 18, 2015). *See also* Jonny Evans, *iOS7: Making Find My Friends Useful and Less Creepy*, COMPUTER WORLD (May 1, 2014), http://www.computerworld.com/article/2476314/apple-ios/ios-7--making-find-my-friends-useful-and-less-creepy.html

[41] YIK YAK, http://www.yikyakapp.com (last visited Mar. 18, 2015). *Who Spewed that Abuse? Yik Yak Isn't Telling,* N.Y. TIMES (Mar. 8, 2015), http://www.nytimes.com/2015/03/09/technology/popular-yik-yak-app-confers-anonymity-and-delivers-abuse.html.

[42] Alyson Shontell, *Here's How Long It Took 15 Hot Startups To Get 1,000,000 Users*, BUSINESS INSIDER (Jan. 8, 2012), http://www.businessinsider.com/one-million-users-startups-2012-1?op=1.

[43] Shea Bennett, *Facebook, Twitter, Instagram, Pinterest, Vine, Snapchat – Social Media Stats 2014*, SOCIALTIMES (June 9, 2014), http://www.adweek.com/socialtimes/social-media-statistics-2014/499230.

the world, and to share and express what matters to them."[44] Facebook has over 1.25 billion monthly users.[45]

On Facebook, users can be "Facebook friends," which allows them access to one another's information, pictures, and Internet posts. Users can privately message one another when they are Facebook friends or without being Facebook friends. Users can link their posts to their Facebook friends by tagging the Facebook friend's username. This alerts the Facebook friend that someone has posted about them. Given the popularity of Facebook, we will use the website's different communication options as the primary examples for each category of communication, though the categories are by no means limited to Facebook and similar websites.

Category 1: Direct

Direct communication occurs when a speaker sends information directly to the target of the communication. On Facebook, a personal message from the speaker to another user would be in this category. Other forums that use direct person-to-person communication include email, personal messages on Google, personal messages on LinkedIn, direct tweets via Twitter,[46] and direct Snapchats.[47]

---

[44] FACEBOOK, https://www.facebook.com/facebook/info?tab=page_info (last visited Mar. 18, 2015).

[45] *Id.*; Emil Protalinski, *Facebook Passes 1.23 Billion Monthly Active Users, 945 Million Mobile Users, and 757 Million Daily Users*, NEXT WEB (Jan. 29, 2014), http://thenextweb.com/facebook/2014/01/29/facebook-passes-1-23-billion-monthly-active-users-945-million-mobile-users-757-million-daily-users/.

[46] A user can tweet directly to another user by starting their message with "@" and then the other person's username. For example, a tweet can be sent directly to President Obama (or, at least, to a staffer who is manning his twitter account) simply by beginning the message with "@BarackObama." The tweet will appear in other users' news feeds if they follow both the sender and President Obama. Users who do not follow both parties can still find and view the tweet by performing a variety of searches, but it will not automatically appear in their news feeds.

[47] Snapchat allows users to send photos directly to another user by using their phone's contacts or by entering a username. *Snapchat Support: Finding and Adding Friends*, SNAPCHAT, https://support.snapchat.com/a/find-friends (last visited Mar. 17, 2015).

Category 2: Tagging

Tagging communication occurs when the speaker takes action to call the communication to the attention of the target. A Facebook example within this category occurs when a user who creates a public post and then attaches the username of a Facebook friend. The "tagged" target receives an automatic notice of the communication by the website. At that point, other users can also see that the target was tagged by the speaker.

Other forums that use tagging communication include Instagram, Vine, Twitter, and LinkedIn. Each of these websites alerts the targets that the speaker tagged them either in a public post or in a post that is visible to the target. The method by which the speaker tags the target is by using an "@" symbol before the name of the target. This triggers the automatic notification to the target.

Category 3: Mutual Forum

Mutual Forum communication does not alert the target that the speaker has posted information about them. Instead, it relies on the fact that the speaker and target are both users of the same online forum and are reasonably likely to see one another's posts during routine usage of the forum. On Facebook, communication in this category would occur if the speaker and the target were Facebook friends, but the speaker did not tag the target of the online post. Because the speaker and the target were using the same forum (Facebook), it is likely that the target would see the post herself. Additionally, if the speaker and the target were both members of the same Facebook group, it is likely that the target would see a post the speaker made on that group's page.

Other social networking websites that allow users to be linked within the forum include LinkedIn, Twitter, Instagram, Vine, and Snapchat. In each of these forums, the target is likely to see postings about themselves because the speaker and target are connected by their association through the social networking website.

Category 4: Likely Discovery

Discovery-based communication does not require the speaker and the target of a particular online post to be users of the same forum. On Facebook, for example, the "Discovery" category would include situations in which the speaker and the target are not Facebook friends. In such situations Tagging communication could not occur because people have to be Facebook friends in order to tag one another—therefore, the target would not receive an automatic alert from the website about the speaker's post. Likewise, the speaker and subject are not using the same forum because they are not Facebook friends, making Mutual Forum communication impossible.

Yet the speaker might still know of or recklessly disregard a substantial likelihood that the subject would discover the speech, enabling what we have dubbed Discovery communication. For example, if the speaker and the target have mutual acquaintances in real life, and the speaker is Facebook friends with many of these real-life acquaintances, then the speaker may have exhibited reckless disregard that the subject would learn about the communications. Indeed, even if the target did not use Facebook at all, the post about the subject could still fall into this category. Similarly, if the speaker knows that the target has a google alert on her name—perhaps because the target has experienced online harassment and abuse in the past, and because the target has written a blog post about using google alerts that the speaker has read—and the speaker still chooses to post threatening comments about the speaker in a forum that he knows a google alert will pick up, this is also a way of communicating with the target.

Factors that make the target more likely to discover the communication include: speaker's knowledge that the target uses the forum; speaker's knowledge that people close to the target use the forum; knowledge that the target has a Google or mention alert on her name[48]; or knowledge that the target frequents the forum—

[48] A Google alert to a sends email notifications any time that Google finds a new posting about any selected topic on the internet. So if someone places a Google alert on their name, it allows people to learn when content including

such as a public blog—if that forum does not require user registration. The inquiry is not a mechanical one; the question is simply whether, taking into account all the relevant circumstances, the speaker knew of or recklessly disregarded a substantial likelihood that the target would find out about the communication.

Category 5: Discovered in Fact

This category contains online speech or behavior by the speaker that the target did *in fact* find out about, but that does not fall into any of the first four categories. Speech in this category might include public comments on a website that the speaker has no reason to know the target reads, or posts on a social networking forum that the speaker has no way of knowing the target uses. It might include speech on the so-called "dark net," where many sites are difficult to access and do not appear with a simple Internet search. It might include speech on protected social media accounts to which neither the target nor any of the target's acquaintances have access. That is, this category includes speech about the target that the speaker would not have expected the target to learn about.

C. "Communication"

In our view, the first four categories of speech we discuss in the previous section—Direct, Tagging, Mutual Forum, and Likely Discovery—should all count as communication for purposes of cyberharassment statutes. The first two categories are relatively straightforward. If a speaker sends a direct message to her target, no matter whether she uses email, instant message, Twitter direct messaging, and so forth, she demonstrates a desire to call the content of the message to the target's attention.[49] Likewise,

---

their name is posted on the web. GOOGLE ALERTS, https://www.google.com/alerts (last visited Mar. 18, 2015).

[49] In *Elonis*, for instance, the defendant made several posts as comments on his ex-wife's sister's posts on Facebook. For example, when the sister posted: "Halloween costume shopping with my niece and nephew should be interesting," Elonis commented, "Tell [their son] he should dress up as matricide for Halloween. I don't know what his comment would entail though. Maybe

by tagging the target of a message, the speaker has taken affirmative steps to ensure that the target receives the message. In both situations, the speaker's choice of medium clearly reveals a desire for the target to learn about the message as well as the decision to convey the message in a way that makes it likely that the target will in fact learn about the message.

The third category—mutual forum communication—should also count as "communication" for purposes of statutes criminalizing cyberharassment. While the speaker has not taken the same affirmative steps to draw the communication to the targets attention as with person-to-person communication or tagging communication, the choice of a mutual forum in itself reveals the speaker's intent and desire for the target to learn of the harasser's comments. That is: why would a speaker post something on Facebook or LinkedIn—knowing that the target of the post also uses the same forum—unless the speaker wanted the target to learn about the communication?

The last form of communication—likely discovery of the communication—should also count. This is the most attenuated means of communication, but we believe that it is also culpable conduct. If the speaker knows that the target of the communication always reads a certain blog, or that she has a google alert on her name that will pick up a comment about her, or that she has friends who will alert her to a Facebook post—the speaker's decision to engage in the communication anyway is best understood as a subtle means of drawing the target's attention to the content of the post. To exempt this category of communication would be to provide an easy end-run around prosecution for speakers who wish to torment or terrify their targets. The speaker can simply post in such a way that they know the target will find about it—thereby accomplishing the goal of disrupting the target's life—yet can evade prosecution by claiming that they used a public forum, regardless whether they knew to a certainty that it was a forum where the target would eventually discover the communication This fourth category of communication is most neglected by current statutes and judicial decision, and as a result we will focus

---

[Tara Elonis's] head on a stick?" United States v. Elonis, 730 F.3d 321 (3d Cir. 2013).

many of our recommendations on the ways statutes should be amended to include this category. To do so is to engage in the essential task of ensuring that our statutes actually reflect the realities of the way people communicate on the Internet.

We do *not* believe that the final category—speech which occurs online but does not rise to the level at which the speaker disregarded a substantial likelihood that the target of the communication would learn about it—should fall within the ambit of cyberharassment statutes. If the subject of a communication does *in fact* learn about a communication—but the author of the communication would not reasonably have anticipated that the subject would do so—it does not evince the intent to disrupt the subject's life in the same manner as the other four modes of communication.

If a speaker has a tumblr,[50] for example, that functions mainly as a diary, and the tumblr is not well-read—for example, it is not followed by any other tumblrs, it has never received any reblogs,[51] no one ever comments on the tumblr, and it appears very low in google search results as the result of limited activity on the page—then absent other circumstances, the author of the tumblr would not expect the subject of a particular post to ever actually read the post. If the subject *did in fact* learn about the post, and experienced the disruption to her life that cyberharassment statutes are designed to guard against, we acknowledge that possibility as an unfortunate byproduct of the need to balance the importance of effective cyberharassment statutes with the importance of not convicting people for engaging in speech that they did not intend to function as harassment, stalking, or bullying.

II. STATE CYBERCRIME LAW AND COMMUNICATION

This Part examines the way that communication is treated within our current cyberharassment regime. We examine the way

[50] Tumblr allows users to create their own blogs where they can post content ("text, photos, quotes, links, music, and videos"). *About*, TUMBLR, https://www.tumblr.com/about (last visited Mar. 17, 2015).

[51] A reblog occurs when one tumblr posts material that has already appeared on another tumblr. Using the tumblr interface, this can be accomplished at the touch of a button.

that "communication" is statutorily defined and judicially interpreted by presenting original empirical research, compiled in Appendix A. Specifically, we survey cyberharassment and cyberstalking statutes in all fifty states and federal law, then summarizes the way these statutes have been interpreted by courts.

A. The Emerging Problem of Cyberharassment

Cyberharassment is a pervasive social problem. A recent poll found that 73% of adults have witnessed someone else being harassed online and 40% have personally experienced harassment.[52] Twenty-five percent of people had seen someone physically threatened online, and 8% had personally experienced online threats.[53] Eighteen percent had seen someone be stalked, and 6% had been stalked themselves.[54] In total, 18% of people had been the targets of "more severe" forms of harassment such as "being the target of physical threats, harassment over a sustained period of time, stalking, and sexual harassment."[55] In particular, young women ages 18-24 experience some of the more severe types of harassment at disproportionately high levels: 26% of women in that age range had been stalked online, and 25% had been the targets of online sexual harassment.[56] 6% of students aged 12–18 reported that they had been victims of cyberbullying.[57]

These statistics are matched by anecdotes that reveal the problematic nature of cyberharassment as well as its pervasiveness,

---

[52] Maeve Duggan, *Online Harassment*, PEW RESEARCH CENTER (Oct. 14, 2014), http://www.pewinternet.org/2014/10/22/online-harassment/.

[53] *Id.*

[54] *Id.*

[55] *Id.* "The U.S. Department of Justice statistics suggest that 850,000 American adults—mostly women—are targets of cyber-stalking each year, and 40 percent of women have experienced dating violence delivered electronically." Marlisse Silver Sweeney, *What the Law Can (and Can't) Do About Online Harassment*, ATLANTIC (Nov. 12, 2014), http://www.theatlantic.com/technology/archive/2014/11/what-the-law-can-and-cant-do-about-online-harassment/382638/.

[56] *Id.*

[57] *Student Reports of Bullying and Cyber-Bullying: Results From the 2009 School Crime Supplement to the National Crime Victimization Survey*, U.S. DEP'T OF EDUC. (Aug. 2011), http://nces.ed.gov/pubs2011/2011336.pdf.

especially although not exclusively for women. In early 2014, Amanda Hess chronicled the experience of a number of women on the Internet who had received threats of violence and other serious harm, including her own experience with a man on Twitter who threatened to decapitate her and with law enforcement's lackluster response.[58] Since Hess's article, a number of other people—mostly women—have shared similar experiences.[59] A particularly disturbing manifestation has emerged recently in the form of GamerGate, in which several prominent women in the gaming community have received threats of death and other violence.[60] Indeed, one of us has substantial experience with online harassment perpetrated by an anonymous individual she never met.[61] As Hess and others have explained, online harassment has serious consequences, particularly for women:

---

[58] Amanda Hess, *Why Women Aren't Welcome on the Internet*, PACIFIC STANDARD (Jan. 6, 2014), http://www.psmag.com/health-and-behavior/women-arent-welcome-internet-72170.

[59] *See, e.g.*, Jill Filipovic, *Let's Be Real: Online Harassment Isn't Virtual for Women*, TALKING POINTS MEMO (Jan. 10, 2014), http://talkingpointsmemo.com/cafe/let-s-be-real-online-harassment-isn-t-virtual-for-women.

[60] *See, e.g.*, Jay Hathaway, *What Is GamerGate, and Why? An Explainer for Non-Geeks*, GAWKER (Oct. 10, 2014), http://gawker.com/what-is-gamergate-and-why-an-explainer-for-non-geeks-1642909080; Zoe Quinn, *5 Things I Learned as the Internet's Most Hated Person*, CRACKED (Sept. 16, 2014), http://www.cracked.com/blog/5-things-i-learned-as-internets-most-hated-person/; Nick Wingfield, *Feminist Critics of Video Games Facing Threats in "Gamer Gate" Campaign*, N.Y. TIMES (Oct. 15, 2014), http://www.nytimes.com/2014/10/16/technology/gamergate-women-video-game-threats-anita-sarkeesian.html?_r=0; Brianna Wu, *Why Gamer Gate Trolls Won't Win*, THE BOSTON GLOBE (Mar. 4, 2015), https://www.bostonglobe.com/magazine/2015/03/04/brianna-why-gamergate-trolls-won-win/l2V0PjfDRSf4Fm6F40i9YM/story.html; Brianna Wu, *No Skin Thick Enough: The Daily Harassment of Women in the Game Industry*, POLYGON (July 22, 2014), http://www.polygon.com/2014/7/22/5926193/women-gaming-harassment.

[61] *See, e.g.*, Nancy Leong, *Identity and Ideas*, FEMINIST LAW PROFESSORS (Nov. 12, 2013), http://www.feministlawprofessors.com/2013/11/identity-ideas/; Nancy Leong, *Anonymity and Abuse*, FEMINIST LAW PROFESSORS (Nov. 19, 2013), http://www.feministlawprofessors.com/2013/11/anonymity-abuse/; Nancy Leong

> But no matter how hard we attempt to ignore it, this type of gendered harassment—and the sheer volume of it—has severe implications for women's status on the Internet. Threats of rape, death, and stalking can overpower our emotional bandwidth, take up our time, and cost us money through legal fees, online protection services, and missed wages.[62]

Given the seriousness of the harm caused by cyberharassment, an effective legal response is important.

These personal stories have also provided powerful evidence that in general law enforcement is poorly educated about online harassment and ill-equipped to deal with most cyberharassment[63] Quantitative data show that cyberharassment is quite rarely prosecuted—for example, Danielle Citron's examination of government data reveals only about twenty-five online threat prosecutions per year[64]—and the host of recent threats against several women made during GamerGate have yet to yield any prosecution.[65]

Despite the pervasiveness of problematic online behavior, online harassment that employs social media platforms is a new problem for the courts. There are a few cases where the victim

---

, Privilege and Passivity, FEMINIST LAW PROFESSORS (Dec. 4, 2013), http://www.feministlawprofessors.com/2013/12/privileging/; Nancy Leong, *Consequences and Conclusions*, FEMINIST LAW PROFESSORS (Dec. 17, 2013), http://www.feministlawprofessors.com/2013/12/consequences-conclusions/.

[62] Hess, *supra* note 58.

[63] *Id.*

[64] Danielle Citron, Elonis v. United States *and the Rarity of Threat Prosecutions*, FORBES (Dec. 3, 2014), http://www.forbes.com/sites/daniellecitron/2014/12/03/united-states-v-elonis-and-the-rarity-of-threat-prosecutions/.

[65] Admittedly the failure to prosecute the people threatening Sarkeesian, Wu, Quinn, and others is not solely attributable to existing laws. Much of the harassment directed at them is clearly criminal under any definition, and the issue is with tracking down the perpetrator electronically or, in some instances, simply getting law enforcement to act. Other conduct, however, is more ambiguous, and both high-profile targets like Sarkeesian, Wu, and Quinn as well as non-famous individuals would benefit from clarification of legal elements including the one we address here—the meaning of communication.

finds success in the courtroom but usually only in instances of severe harassment. The most common form of harassment that the court holds to be cyberharassment is the public release of sexually explicit photographs and videos of the victim.[66] The courts are also likely to find guilt where the harasser has released the victim's private information.[67] It is rare that courts will find guilt where there is only one instance of a harassing action or if that action is not severe.[68]

Yet it should be noted that no matter how severe the harassment, a court cannot take action if the statute is not properly constructed to protect the victim. This can be a statute being found unconstitutional.[69] Or, what our Article focuses on, if the statute does not have a clear definition of what it means to communicate.

---

[66] *See e.g.*, United States v. Sayer, 748 F.3d 425 (1st Cir. 2014) (defendant made sexual Craiglist ads, Facebook accounts, and posted sexual acts of the victim on pornography sites); United States v. Osinger, 753 F.3d 939 (9th Cir. 2014) (defendant created a false Facebook account featuring sexually explicit photographs of the victim, and sent emails to the victim's co-workers and friends also containing explicit photographs); People v. Kucharski, 996 N.E.2d 906 (Ill. App. 2013) (defendant hacked his ex-girlfriend's MySpace page and posted a photo of her bending forward wearing only a thong and posted her phone number and address).

[67] In fact, the first cyberstalking conviction in California was based on the release of personal information. The defendant "told numerous men everything from the address of [the victim's] apartment to her physical description, her phone number and how to bypass her home security system." Greg Miller & David Maharaj, *N. Hollywood Man Charged in 1st Cyber-Stalking Case*, LOS ANGELES TIMES (Jan. 22, 1999), http://articles.latimes.com/1999/jan/22/news/mn-523.

[68] As an example of one success, the Ohio court found a defendant guilty where she had posted one comment that the victim "molested a little boy." State v. Ellison, 900 N.E.2d 228 (Ohio Ct. App. 2008). Notably Ohio had a very expansive cyberharassment statute: "No person shall make or cause to be made a telecommunication . . . with purpose to abuse, threaten, or harass another person." *Id.* (citing R.C. 2917.21(B)).

[69] *See, e.g.*, People v. Marquan, 19 N.E.3d 180 (N.Y. 2014) (defendant had posted information about his classmates' sexual practices on Facebook, but the court held that the law was overbroad because it had "a wide array of applications that prohibit types of protected speech far beyond the cyberbullying of children"); U.S. v. Cassidy, 814 F.Supp.2d 574 (D. Md. 2011) (defendant had made a twitter account and tweeted hundreds of messages about the victim and was chaged under the interstate stalking statute, which was found to be an unconstitutional content-based restriction on speech as applied to the defendant).

For example, in *People v. Barber*, the defendant posted nude photos of his ex-girlfriend online and sent those photos to her employer, all without her consent.[70] New York, as a state without a cyberharassment statute with a reference to online communication, charged Barber with aggravated harassment in the second degree.[71] While the court found Barber's actions "reprehensible," it was unable to hold him accountable because the material was not "communicated directly" with the victim.[72] The court found it insufficient that the victim saw that he had posted the photos online and had seen the email to her employer.[73]

While statistics of cyberharassment trials, convictions, and pleas are non-existent at the worst and incomplete at the best, it is universally acknowledged that "it is a paltry number given the estimated number of [cyberharassment] cases a year."[74] Both a cause and a consequence of the lack of prosecution of cyberharassment is that many important issues remain unaddressed by the courts. As a result, law enforcement agencies may remain unsure of what constitutes a crime and prosecutors may hesitate to press charges, with the result that a great deal of problematic online behavior remains unpunished. One element notably lacking in clarity is the meaning of "communication," which we address in subsequent sections of this Article.

---

[70] People v. Barber, 992 N.Y.S.2d 159 (2014). This phenomenon has become known as "revenge porn," where a person will post sexually explicit photos or video of their ex-significant other, intending to publically humiliate them. *See* Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. (forthcoming 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2368946.

[71] Along with two other charges that were dismissed on other grounds. *Barber*, 992 N.Y.S.2d at 159.

[72] *Id.*

[73] *Id.*

[74] Danielle Citron, *United States v. Elonis and the Rarity of Threat Prosecutions*, FORBES (Dec. 03, 2014), http://www.forbes.com/sites/daniellecitron/2014/12/03/united-states-v-elonis-and-the-rarity-of-threat-prosecutions/.

B. Criminalizing Cyberharassment

In this section, we evaluate the way that cyberharassment is currently treated under criminal law. We first consider threshold issues of constitutionality. We then present an original empirical survey of state cyberharassment laws based on the way communication is defined in those statutes, and discuss the way that courts have interpreted these statutes.

1. Constitutionality

Cyberharassment statutes must survive constitutional scrutiny. The Supreme Court maintains that "basic principles of freedom of speech and press, like the First Amendment's command, do not vary when a new and different medium for communication appears."[75] Nonetheless, the Court has also made clear that developments in technology influence the appropriate interpretation of constitutional rights.[76] The First Amendment, then, need not be intentionally blind to the real differences in the way the Internet has changed the way we interact with one another.

This constitutional backdrop makes clear that cyberharassment can be criminalized via carefully drawn statutes. The Supreme Court has consistently classified emotionally distressing or outrageous speech as protected, especially where that speech touches on matters of political, religious or public concern.[77] But speech integral to criminal conduct is a long-established category of unprotected speech.[78] For example,

[75] United States v. Cassidy, 814 F. Supp. 2d 574 (D. Md. 2011).

[76] *See, e.g.*, Riley v. California 134 S. Ct. 2473 (2014) (holding that police may not execute a warrantless search of a cell phone incident to an arrest, and, more generally, acknowledging evolving technology as consideration in constitutional analysis); Kyllo v. United States, 121 S. Ct. 2038 (2001). *See also* [redacted], *Constitutional Rights in the Digital Age*, HUFFINGTON POST (July 19, 2014), http://www.huffingtonpost.com/nancy-leong/constitutional-rights-in-first-amendment_b_5601216.html.

[77] United States v. Sayer, 748 F.3d 425 (1st Cir. 2014).

[78] Giboney v. Empire Storage & Ice Co., 69 S. Ct. 684 (1949); *Sayer*, 748 F.3d at 425.

"speech is not protected by the First Amendment when it is the very vehicle of the crime itself" such as in crimes of perjury, bribery, extortion and threats, and conspiracy.[79] Likewise, when speech contains "true threats," as the speech criminalized by cyberharassment statues often does, that speech is also unprotected.[80] Although the Supreme Court has never clearly defined what a true threat is—it may do so this term in *Elonis v. United States*[81]—lower courts have adopted a variety of tests.[82]

Challengers to cyberharassment statutes therefore raise two primary arguments: (1) that the statute is void for vagueness; and (2) that the statute violates the First Amendment by punishing protected speech.

A criminal law may be unconstitutionally vague for either of two independent reasons. First, the statute may fail to provide the kind of notice that would enable a person of ordinary intelligence to understand what conduct is prohibited. Second, a statute may fail to provide explicit standards for those who apply it, thus authorizing or even encouraging arbitrary and discriminatory enforcement.[83] Invalidating vague statutes avoids: punishing people for behavior that they could not have known was illegal; subjective enforcement of laws based on arbitrary and

---

[79] United States v. Varani, 435 F.2d 758 (6th Cir. 1970).

[80] United States v. Watts, 349 U.S. 705 (1969).

[81] Elonis v. United States, 730 F.3d 321 (3d Cir. 2013), *cert. granted*, 134 S. Ct. 2819 (2014).

[82] For example, some courts consider a series of factors in determining whether speech constitutes a true threat, including (1) the reaction of the recipient of the speech; (2) whether the threat was conditional; (3) whether the speaker communicated the speech directly to the recipient; (4) whether the speaker had made similar statements in the past; and (5) whether the recipient had reason to believe the speaker could engage in violence. *See, e.g.*, Jones v. State of Arkansas, 64 S.W.3d 728, 735 (Ark. 2002) (determining that a student giving his rap song threatening violence to another student was a true threat). Other courts use a "reasonable person" test, explaining: "if a reasonable person would foresee that an objective rational recipient of the statement would interpret its language to constitute a serious expression . . . [then] the message conveys a 'true threat.'" U.S. v. Miller, 115 F.3d 361 (6th Cir. 1997), *cert. denied*, 522 U.S. 883 (1997).

[83] People v. Kucharski, 996 N.E.2d 19 (Ill. App. 2013).

discriminatory enforcement by government officers; and any chilling effect on the exercise of First Amendment freedoms.[84]

The test for vagueness "is necessarily a practical rather than hyper-technical one," and when a statute fails to provide an explicit definition, the court may resort to ordinary meaning and common sense, considering whether the statute "conveys sufficiently definite warning as to the proscribed conduct when measured by common understanding and practices."[85]

Analysis of the federal cyberstalking statute demonstrates the way these constitutional principles play out in practice. The statute prohibits "engaging in a course of conduct by use of interactive computer services with the intent to kill injure, harass, or intimidate another."[86] The federal cyberstalking statute is not unconstitutionally vague because the statute provides sufficient notice of the respective prohibitions and citizens need not guess what terms such as "harass" and "intimidate" mean.[87] Further, the government is only required to show that the totality of the defendant's conduct "evidenced a continuity of purpose" to achieve the criminal end.[88]

For example, in *United States v. Osinger*, the defendant's threats, creation of a false Facebook page with sexually explicit photographs of the victim, and emails to the victim's co-workers and friends containing explicit photographs evinced the defendant's "intent to . . . cause substantial emotional distress . . ."[89] Thus, the defendant's unrelenting harassment and intimidation of the victim

---

[84] United States v. Osinger, 753 F.3d 939 (9th Cir. 2014).

[85] United States v. Shrader, 675 F.3d 300 (4th Cir. 2012).

[86] 18 U.S.C. § 2261A (2012).

[87] *Id.*; *Osinger*, 753 F.3d at 939; United States v. Shepard, 12-10253, 2014 WL 2750117 (9th Cir. June 18, 2014); People v. Sucic, 928 N.E.2d 1231 (Ill. App. 2010); United States v. Sayer, 748 F.3d 425 (1st Cir. 2014); United States v. Bowker, 372 F.3d 365, 378–79 (6th Cir. 2004) (vacated on grounds unrelated to constitutionality of cyberstalking statute).

[88] The statute does not impose a requirement that the government prove that each act was intended in isolation to cause serious distress or fear of bodily injury to the victim. United States v. Bowker, 372 F.3d 365 (6th Cir. 2004); *Shrader*, 675 F.3d at 300.

[89] *Osinger*, 753 F.3d at 939.

was not based on conduct that he "could not have known was illegal" because of vagueness. [90]

Complementing the Ninth Circuit's decision in *Osinger*, New York and the Second Circuit have held that statues which criminalize intentional communication with the intent to "alarm or annoy" are unconstitutional on both freedom of speech and vagueness grounds.[91] In *Vives v. City of New York*, the court held that determining what language would classify as alarming or annoying was too vague because the determination would be rely on the person receiving the communication.[92]

In contrast, the Sixth Circuit held that any vagueness associated with the word "annoy" was mitigated by the fact that the meanings of "threaten" and "harass" can easily be ascertained and have generally accepted meanings.[93] The court suggests that the words annoy, abuse, threaten or harass should be read together to be given similar meanings.[94]

The Supreme Court has not addressed this specific language issue. Lower courts, however, have either taken the inclusion approach or have simply read the word "annoy" out of the statute, holding that the remainder is sufficiently specific to survive scrutiny.

A criminal law may violate the freedom of speech if it restricts general speech that is not a "true threat" or "fighting words."[95] The federal cyberstalking statute does not prohibit protected speech because it is the conduct rather than the speech

---

[90] *Id.*

[91] People v. Golb, 23 N.Y.3d 455 (N.Y. 2014); Vives v. City of New York, 305 F. Supp. 2d 300 (S.D.N.Y. 2003)

[92] Additionally, the court found the intent to "annoy or alarm" to be protected under the Constitution because communication that alarms or annoys does not constitute fighting words or true threats and, therefore, that criminalizing such speech is "utterly repugnant to the First Amendment of the United States Constitution." *Golb*, 23 N.Y.3d at 455; *Vives*, 305 F. Supp. 2d at 300.

[93] *Bowker*, 372 F.3d at 365.

[94] *Id.*

[95] Cohen v. California, 403 U.S. 15, 20 (1971) (fighting words); Watts v. United States, 394 U.S. 705, 708 (1969) (true threats).

that is prohibited.[96] Most, if not all, of cyberharassment statutes' legal applications are to conduct that is not protected by the First Amendment.[97] It is difficult to imagine what constitutionally-protected speech would fall under the cyberharassment statutory prohibitions because the statutes require both malicious intent on the part of the defendant and substantial harm to the target.[98]

The federal cyberstalking statute specifically criminalizes "a course of *conduct* that . . . causes . . . substantial emotional distress" and provides "the term 'course of conduct' means a pattern of conduct composed of two or more acts, evidencing a continuity of purpose."[99] Thus, the proscribed acts of cyberharassment are tethered to the underlying criminal conduct and not to speech.[100] The element of a threat is also an integral part of the offense of cyberharassment.[101] Therefore, that element narrows the punishable behavior such that the defendant must "knowingly and without lawful justification" specifically intend to "harass" the target by transmitting the threat.[102]

Only one federal district court case has held that the indictment of a defendant under the federal cyberstalking statute violated the First Amendment.[103] In *United States v. Cassidy*, the prosecution indicted an individual for tweets and blog posts that were critical of a "well-known religious figure" and that questioned the subject's "character and qualifications as a religious leader."[104] In the specific context of the particular indictment, the court held that the indictment violated the First Amendment, but explicitly declined to consider whether the cyberstalking statute was facially invalid.[105]

---

[96] "Intimidating conduct serves no legitimate purpose and merits no first amendment protection." State v. Hemmingway, 825 N.W.2d 303 (Wis. App. 2012).

[97] *Bowker*, 372 F.3d at 365.

[98] United States v. Petrovic, 701 F.3d 849 (8th Cir. 2012).

[99] 18 U.S.C.A. § 2261A (emphasis added).

[100] United States v. Osinger, 753 F.3d 939 (9th Cir. 2014).

[101] Threats are not protections of the first amendment. People v. Sucic, 928 N.E.2d 1231 (Ill. App. 2010).

[102] *Id.*

[103] United States v. Cassidy, 814 F. Supp. 2d 574 (D. Md. 2011).

[104] *Id.* at 583.

[105] *Id.* at 587–88.

Thus, cyberharassment and cyberstalking statutes can be drafted in a manner that complies with the requirements of the First Amendment. And, in general, the federal courts have found that the federal cyberstalking statute is drafted in such a way.

2. Communication in cyberharassment statutes

This section examines the way that "communication" is currently statutorily defined. All cyberharassment statutes have three elements: intentional mens rea with respect to the making of the communication, threatening or harassing communication, and victim knowledge of the communication. We divided the current statutes into five categories based on how communication is statutorily defined. A chart containing all the statutes is appended to this Article.[106]

Category 1: No Reference to Online Communication

Some states do not explicitly refer to online communication in any criminal statutes. This is true in six states (Delaware, Maine, Nebraska, New Jersey, New Mexico, and New York).

Category 2: Undefined "Electronic Communication"

Sixteen states (Alabama, Alaska, Connecticut, Florida, Hawaii, Idaho, Indiana, Iowa, Missouri, Montana, North Dakota, Rhode Island, South Dakota, Utah, Vermont, and Virginia) criminalize threatening "electronic communication," but do not define that communication.[107] In Category 2, only Florida, Rhode Island and Virginia have separate "Cyberstalking" or "Harassment

[106] *See* Appendix A.

[107] ALA. CODE § 13A-6-90.1 (2015); ALASKA STAT. § 11.41.270 (2015); CONN. GEN. STAT. § 53a-182b (2015); FLA. STAT. § 784.048 (2015); HAW. REV. STAT. § 711-1106 (2015); IDAHO CODE ANN. § 18-7906 (2015); IND. CODE § 35-45-2-2 (2015); IOWA CODE § 708.7 (2015); MO. REV. STAT. § 565.225 (2015); MONT. CODE ANN. § 45-5-220 (2015); N.D. CENT. CODE § 12.1-17-07 (2015); R.I. GEN. LAWS § 11-52-4.2 (2015); S.D. CODIFIED LAWS § 22-19A-1 (2015); UTAH CODE ANN. § 76-5-106.5 (2015); VT. STAT. ANN. 13 V.S. 1602 (2015); VA. CODE ANN. § 18.2-152.7:1 (2015).

by Computer" statutes. All of the other states in Category 2 include electronic communication within the "Harassment" or "Stalking" statute.

Category 3: Statutorily-Specified Communication

Nine states (Arizona, Colorado, Georgia, Kansas, Kentucky, New Hampshire, Pennsylvania, Washington, and West Virginia) criminalize and define threatening electronic communication with specific examples but omit many types of communication in the definition. For example, Arizona defines electronic communication as only "a wire line, cable, wireless or cellular telephone call, a text message, an instant message or electronic mail."[108]

Category 4: All Direct Victim Communication:

Twelve states (California, Louisiana, Maryland, Massachusetts, Mississippi, North Carolina, Ohio, Oklahoma, Oregon, Tennessee, Texas, and Wyoming) and federal law define threatening communication to include all types of communication, but require that the threatening language be directed at a particular target.[109] What it means for the language to be directed at a person varies from state to state.

For example, Louisiana defines electronic communication as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature, transmitted in whole or in part by wire, radio, computer, electromagnetic, photoelectric, or photo-optical system, use of the Internet, a computer, a facsimile machine, a pager, a cellular telephone, a video recorder, or other electronic

[108] ARIZ. REV. STAT. ANN. § 13-2916 (2015).

[109] 18 U.S.C.A. § 2261A (2012); ARIZ. REV. STAT. ANN. § 13-2916 (2015); CAL. PENAL CODE § 653m (West 2015); LA. REV. STAT. ANN. § 14:40.3 (2015); MD. CODE ANN., Crim. Law § 3-805 (2015); MASS. GEN. LAWS 265 § 43 (2015); MINN. STAT. § 609.749 (2015); MISS. CODE ANN. § 97-45-15 (2015); N.C. GEN. STAT. § 14-196.3 (2015); OHIO REV. CODE ANN. § 2903.211 (West 2015); OKLA. STAT. tit. 21, § 1172 (2015); OR. REV. STAT. § 166.065 (2015); TENN. CODE ANN. § 39-17-308; TEX. PENAL CODE ANN. § 42.07 (2015); WYO. STAT. ANN. § 6-2-506 (2015).

means."[110] This communication must, however, be "sent to a person identified by a unique address or address number and received by that person."[111]

Other state statutes take a similar approach. For example, Mississippi criminalizes all types of electronic mail or electronic communication "with another, repeatedly, whether or not conversation ensues."[112] Similarly, although Wyoming does not have a separate cyberstalking statute, it criminalizes "communicating, anonymously or otherwise, or causing a communication with another person by verbal, electronic, mechanical, telegraphic, telephonic or written means *directed at a specific person"* in its stalking statute.[113]

Category 5: Reasonable Victim's Knowledge of Communication

Seven states (Arkansas, Illinois, Michigan, Minnesota, Nevada, South Carolina, and Wisconsin) have stalking or harassment statutes that do not require a statement to be made directly to the person.[114] Instead, they criminalize any statement made that would cause a reasonable recipient to feel threatened. For example, Nevada criminalizes any "display or distribute of information in a manner that substantially increases the risk of harm or violence to the victim."[115] Similarly, although Minnesota does not have a separate cyberstalking statute, the stalking statute criminalizes "any communication made through any available technologies or other objects which the actor knows or has reason to know would cause the victim under the circumstances to feel frightened, threatened, oppressed, persecuted, or intimidated"[116] Category 5 is different from Category 1 because the language of

---

[110] LA. REV. STAT. ANN. § 14:40.3 (2015).

[111] *Id.*

[112] MISS. CODE ANN. § 97-45-15 (2015).

[113] WYO. STAT. ANN. § 6-2-506 (2015) (emphasis added).

[114] ARK. CODE ANN. § 5-71-217 (2015); ILL. COMP. STAT. 720 ILCS 5/12-7.5 (2015); MICH. COMP. LAWS § 750.411s (2015); MINN. STAT. § 609.749 (2015); NEV. REV. STAT. § 200.575 (2015); S.C. CODE ANN. § 16-3-1700 (2015); WIS. STAT. § 947.0125 (2015).

[115] NEV. REV. STAT. § 200.575 (2015).

[116] MINN. STAT. § 609.749 (2015).

the statutes in Category 1 does not include online communication and the language of the statutes in Category 5 explicitly does.

3. Communication in cyberharassment cases

This section explains how courts have defined the phrase "communication" in cases involving online behavior. Just as different cyberstalking statutes define communication differently, case law defining communication varies based on the statutory requirements.

All courts have held that emails sent to the target satisfy the requirement of "direct communication with the victim."[117] Moreover, that an Internet message can be a "true threat" not protected by First Amendment without being sent directly to victim.[118]

In New York, a state court has gone a step further and held that messages in a newsgroup, similar to a blog, also qualified as a direct communication. In *People v. Munn*, the defendant posted a message to kill a police sergeant and all other members of the NYPD.[119] The message was in a "newsgroup," posted daily and read by a group of regular participants, but open to be read by anyone with a computer and "on line" capabilities.[120] The court found that defendant's posting on an Internet newsgroup with the complainant's name included then transformed the communication to one not only intended for the general public, but specially generated to be communicated to the complainant.[121] Therefore, the court found that communications in a public newsgroup

[117] However, Florida held changing email password and appropriating emails is not cyberstalking because it is not electronic communication directed at the victim, as required by the statute. Young v. Young, 96 So. 3d 478 (Fla. Dist. Ct. App. 2012).; M.G. v. C.G., 862 N.Y.S.2d 815 (N.Y. Fam. Ct. 2008); People v. Munn, 688 N.Y.S.2d 384 (N.Y. Crim. Ct. 1999); Barson v. Com., 726 S.E.2d 292 (Va. 2012) (reversed on other grounds).

[118] People v. Diomedes, 13 N.E.3d 125, (Ill. App. 2014); *see also* Elonis v. United States, 730 F.3d 321 (3d Cir. 2013), *cert. granted*, 134 S. Ct. 2819 (2014).

[119] People v. Munn, 688 N.Y.S.2d 384 (Crim. Ct. 1999).

[120] *Id.*

[121] *Id.*

message is considered written communication directed at the person for purposes of harassment.[122]

But other courts' failure to use a definition of communication that reflects the way people actually use the Internet results in a failure to convict individuals who have clearly engaged in online behavior that terrorized their victims.

In *State v. Ellison*, for example, a case arising in Ohio, the defendant posted a picture of the target to MySpace with a caption that the target liked to molest little boys.[123] The MySpace post was available to the public but not sent directly to the target.[124] The relevant Ohio statute prohibited "telecommunication with the purpose to abuse, threaten, or harass another person,"[125] and before the trial court, the defendant was convicted of "Harassment by Telecommunication."[126]

On appeal, however, the Ohio Court of Appeals determined that "the statute creates a specific-intent crime: the state must prove the defendant's specific purpose to harass."[127] The court held that direct contact with the target was not necessary, but that the state must prove the intent of the defendant was to harass the target.[128] The defendant claimed, and the court agreed that the intent of the defendant was to warn the public of the target's character and not to harass the target.[129] The court reversed the conviction.[130]

Ellison reveals a misplaced focus on the intent of the defendant rather than—in keeping with the purpose of cyberharassment statutes in general, which is to avoid disruption and fear in innocent citizens' lives—a focus on whether a threatening or severely distressing message was communicated to the target. Such communication should be the focus: after all, the

---

[122] *Id.*
[123] State v. Ellison, 900 N.E.2d 228 (Ohio App. 2008).
[124] *Id.*
[125] *Id.*
[126] *Id.*
[127] *Id.*
[128] *Id.*
[129] *Id.*
[130] *Id.*

point of cyberharassment statutes is to prevent the harms arising from such communication.

In other situations, prosecutors have simply declined to press charges because of the inadequate statutory tools available to them. In September of 2006, Lori Drew became concerned that Megan Meier, a 13 year old neighbor, was spreading rumors about her daughter. Drew created a false MySpace account in the name of "Josh Evans."[131] Drew used the MySpace account pretend to be a 16-year-old boy and flirt with Meier.[132] "Josh Evans" began sending Meier negative messages on October 15 and continuing throughout the next day. On October 16, 2006, "Josh Evans" sent Meier a message to the effect that the world would be a better place without her.[133] Additional MySpace members whose profiles reflected links with the "Josh Evans" profile also began to send Meier disparaging messages.[134] Subsequently, Meier's mother discovered that her daughter had hanged herself in her bedroom closet.[135] Missouri prosecutors did not press charges because they could not prove Drew intended to cause emotional distress.[136] Yet again, this focus is misplaced. The disruption to Meier's life is the harm that the statute is intended to prevent, and as a result the focus of the prosecution should remain on the nature of the communication.[137]

---

[131] *The Story of Megan Meier*, MEGAN MEIER FOUNDATION, http://www.meganmeierfoundation.org/megans-story.html (last visited Mar. 18, 2015).

[132] *Id.*

[133] *Id.*

[134] *Id.*

[135] *Id.*

[136] *Prosecutor: No Criminal Charges in MySpace Suicide*, FOXNEWS (Dec. 03, 2007), http://www.foxnews.com/story/2007/12/03/prosecutor-no-criminal-charges-in-myspace-suicide/.

[137] A similar example of unprosecuted cyberharassment occurred in Tampa, Florida in 2012. There, an ex-mistress, Paula Broadwell sent anonymous threatening emails to the wife of the person with whom she was had an affair. In the emails, Broadwell touted her military background in a threatening manner and boasted of having "powerful" friends. Matthew Lysiak, *Menacing Emails Sent by David Petraeus' Ex-Mistress Paula Broadwell to Socialite Jill Kelley Promised to Make the Apparent Rival 'Go Away,'* DAILYNEWS (Nov. 20, 2012), http://www.nydailynews.com/news/national/broadwell-emails-kelley-sinister-previously-reported-article-1.1204956. The target saw the emails as death

Finally, the recent passage of statutes that strive to criminalize the phenomenon known as "revenge porn" also reveal the deficiencies in current cyberharassment statutes.[138] Revenge porn—more accurately known as non-consensual pornography—consists of online posting of nude pictures of another person without that person's consent.[139] Often, although not always, the person who posts the pictures is an angry ex-partner.[140] Some websites exist solely for the purpose of posting non-consensual pornography.[141] Posting such pictures is often a mechanism of communication: for example, the website MyEx.com invites users to post links to the email address, phone number, Facebook page, LinkedIn page, and other information of people depicted in uploaded photos.[142] The inevitable result is that other users often send threatening and harassing messages to the person depicted in the photos, with the result that the person depicted finds out about the pictures and, often, realizes who uploaded them. In many instances, it is difficult to imagine a clearer way to communicate hatred or contempt to the person depicted in the photos. Yet the

---

threats, specifically one in which Broadwell vowed to "make [her] go away." But prosecutors never filed charges, again because of the focus on intent rather than the focus on communication and the disruption it causes. *Paula Broadwell Won't Face Cyberstalking Charges in Petraeus Scandal*, NBCNEWS (Dec. 18, 2012), http://investigations.nbcnews.com/_news/2012/12/18/15995676-paula-broadwell-wont-face-cyberstalking-charges-in-petraeus-scandal.

[138] Citron & Franks, *supra* note 70.

[139] *Id.*

[140] *Id.*

[141] *See, e.g.*, *MyEx.com Get Revenge! Naked Pics of Your Ex*, MYEX.COM, http://www.myex.com (last visited Mar. 18, 2015). Another popular site, IsAnybodyUp.com, averaged 30 million views a month at its peak. Daniel Kreps, *Revenge-Porn Site Owner Hunter Moore Pleads Guilty, Faces Prison Time*, ROLLINGSTONE (Feb. 20, 2015). IsAnybodyUp.com shut down in 2012, as a result of intense public pressure. *Id.* Note that while the website founder was indicted and eventually pled guilty, it was not on charges related specifically to the protection of revenge-porn victims, "as many states' cyber-laws still haven't been revamped to confront the relatively new phenomenon." Jessica Roy, *Revenge-Porn King Hunter Moore, the 'Most Hated Man on the Internet,' Is Going to Jail*, N.Y. MAG. (Feb. 19, 2015), http://nymag.com/daily/intelligencer/2015/02/revenge-porn-hunter-moore-jail.html.

[142] *MyEx.com Get Revenge! Naked Pics of Your Ex*, MYEX.COM, http://www.myex.com (last visited Mar. 18, 2015).

fact that cyberharassment statutes fail to cover posting such pictures reveals the shortcomings of such statutes and their inadequate focus on communication.

III. UPDATING THE MEANING OF "COMMUNICATION"

This Part first briefly articulates the problems associated with the lack of a clear and up-to-date statutory definition of "communication." It then proposes a definition that can be used by both legislatures and courts, and offers concrete examples that demonstrate why the definition is sensible.

A. Statutory Proposal

As we have explained, the myriad ways in which people interact on the Internet require a careful and accurate definition of "communication" in cyberharassment statutes. As we have argued, such a definition should include any form of online behavior that a reasonable person knew or recklessly disregarded a reasonable likelihood that the target would learn about the behavior.

Currently, many cyberharassment statutes—including the federal statute—define cyberharassment around the "use" of an electronic communications device to engage in a "course of conduct." We think that rephrasing the statute and others like it to criminalize communication that warrants punishment correctly places the focus on the interaction between the speaker and the target.

We propose the following language to describe the interaction between the speaker and the target:

> *An individual commits the crime of cyberharassment when he or she knowingly and repeatedly engages in online communication about the target in a manner that a reasonable person would find threatening or would cause severe emotional distress, and that the target did in fact find threatening or severely emotionally distressing.*
> *(a) "Communication" is defined as speech or conduct using any electronic medium when the individual knew or recklessly disregarded a substantial likelihood that the target would learn about the speech or conduct;*
> *(b) "Repeatedly" means more than once.*

The first part of the statute closely tracks the language in existing cyberharassment statutes whose constitutionality courts have upheld. By requiring that the speech is either threatening or severely emotionally distressing, the statute avoids criminalizing speech that is merely annoying or disparaging—that is, it focuses on speech whose prohibition, as Justice O'Connor articulated in *Virginia v. Black*, "protect[s] individuals from the fear of violence" and "from the disruption that fear engenders," in addition to protecting people "from the possibility that the threatened violence will occur."[143]

Key to our project is section (a), which defines communication. We employ a definition that includes only speech or conduct when the perpetrator either knew there was a substantial likelihood that the target would find out about the speech or conduct, or recklessly disregarded a substantial likelihood that the target would find out about the speech. This definition goes to the heart of the harms caused by threatening or distressing communications on the Internet: if the perpetrator knows or disregards a substantial likelihood that the target will find out about a particular instance of online behavior, the behavior is

[143] Virginia v. Black, 538 U.S. 343, 459–60 (2003).

closely akin to the type of direct communication (letters; phone calls) that were criminalized in the pre-Internet world. In the next section, we explain how our statute—and its careful definition of communication—will apply to a range of behavior on the Internet.

B. Examples

Finally, we turn to the task of articulating how our proposed definition of communication would play out in the context of several examples spanning a range of social media platforms. In each instance, we demonstrate that the speaker knew or recklessly disregarded the reasonable likelihood that the subject would learn of the speech, and, therefore, that the activity should count as communication. We demonstrate not only that the test works across existing platforms, but also that it can accommodate new platforms as well.

Example 1: Allison is friends with Brenda on Facebook. Allison writes a post about Brenda on Facebook that is visible to all of Allison's Facebook friends.

This example qualifies as communication under our definition. Even if Allison does not tag Brenda in the post, people often see their friends' posts on Facebook while browsing their news feeds—the average American now spends forty minutes a day on Facebook,[144] and some check far more frequently.[145] Additionally, Allison and Brenda's mutual friends would likely inform Brenda of the post, or ask her questions about it, if the post was at all interesting or salacious. In the unlikely event that Allison believed that Brenda would not find out about the post, Allison

[144] Joshua Brustein, *Americans Now Spend More Time on Facebook Than they Do on Their Pets*, BLOOMBERG (July 23, 2014), http://www.bloomberg.com/bw/articles/2014-07-23/heres-how-much-time-people-spend-on-facebook-daily.

[145] Stephen Marche, *Is Facebook Making Us Lonely?*, ATLANTIC (Apr. 2, 2015), http://www.theatlantic.com/magazine/archive/2012/05/is-facebook-making-us-lonely/308930/ ("Among 18-to-34-year-olds, nearly half check Facebook minutes after waking up, and 28 percent do so before getting out of bed.").

would have had to recklessly disregard the time and manner in which most people use Facebook, as well as the likelihood that mutual friends would alert Brenda of the post's existence. A post made with such reckless disregard should count as communication.

Example 2: Cesar and Dave are not friends on Facebook, but they have many mutual Facebook friends. Cesar writes a post about Dave.

This example likewise qualifies as communication. Even though Dave may never see the Facebook posting himself, the many mutual friends of Cesar and Dave would make it likely that Dave would find out about it. On Facebook, it is easy to tell how many mutual friends one shares with another person, regardless whether one is friends with that person. Thus, Cesar would have to recklessly disregard the readily-available information that he and Dave had multiple mutual friends in order to believe that none of the mutual friends would alert the subject to the communication.

Example 3: Ed writes one post about Frida on Reddit.

Reddit is a website that bills itself as "the front page of the Internet."[146] It is divided into a large number of forums, all of which are publicly accessible and in any of which anyone can write a post of any length. The site constantly updates itself, making certain content more visible or less visible depending on the number of views the content has received and the time since the posting. All posts are publicly available until the post is removed by the creator.

If Ed writes one post about Frida on Reddit, his post should not count as communication because it is a single incident and Frida is unlikely to find out about it. If the isolated post is the only thing Ed has ever written about Frida, neither Frida nor people close to her would have any reason to be on alert for a posting about her. Further, if Ed's post was the only thing he had written about Frida, it is unlikely that even if someone close to Frida saw

[146] *Reddit: The Front Page of the Internet*, REDDIT, http://www.reddit.com (last visited Mar. 18, 2015).

the blog that they would tell her about it. In this instance, Ed has not recklessly disregarded a reasonable likelihood that Frida would find out about the Reddit post.

Example 4: Gary creates a blog dedicated to writing disparaging and threatening posts about Holden.

Anyone with access to the Internet can create a blog. While some blogs cost money to create and maintain, many platforms, such as Tumblr, Blogspot, and Blogger, allow people to create blogs for free. The settings on a particular blog may allow comments from viewers, or the blog may exist only as a forum for the author of the blog. While blogs may be public or private, a public blog can be viewed by anyone and the posts are available until they are taken down by the owner of the blog.

A blog dedicated to negative commentary about Holden should count as communication so long as the blog is public. Most people google themselves occasionally in order to know what is on the Internet about them. Some even have google or mention alerts on their names. And other people—potential dates; potential employers—likewise google people. Given all of these possible avenues for learning about the blog via Internet searches, Gary's creation of the blog about Holden should count as communication because it is reasonably likely that Holden would find out about the blog.

Example 5: Ida creates a Craigslist ad that includes Jaliah's phone number and address and states that Jaliah is willing to have sex for money.

Craigslist is a website that allows anyone to post an ad that is made available to the public online. The website categorizes the postings by topic, such as "For Sale," "Wanted," "Housing," "Casual Encounters," and so forth. The ads are visible to anyone on the Internet, although in some instances they expire after a specified length of time such as a week. Posts often include contact information for the party who has (supposedly) created the advertisement.

Ida's Craigslist posting about Jaliah counts as communication. Even though Jaliah might not find the Craigslist posting herself, the posting itself would solicit responses from those who do see it. Jaliah would likely find out about the posting from people who call her on the phone or even come to her house. Ida's posting of Jaliah's contact information would establish knowledge by Ida of a reasonable likelihood that Jaliah would be contacted and, therefore, that Jaliah would discover the posting.

Example 6: Keith and Leah both use Twitter. Keith writes several public tweets about Leah threatening to harm her and her family. He mentions Leah by her full name but does not include her Twitter handle. Keith and Leah each have about 500 Twitter followers, but they do not have any Twitter followers in common.

While this is a close case, we believe that this example should qualify as communication. Admittedly Keith has not used the "@" symbol to call Leah's attention to his tweets, and the lack of mutual followers diminishes the likelihood that anyone will mention the tweets to Leah. With that said, there are a number of ways that Leah could find out about the tweets, such that she is reasonably likely to do so and the tweets should count as communication. Given that the tweets are public, Leah could find the tweets by googling her name. She could also find them by using Twitter's search function to search for her name. If the tweets are threatening, it is possible that one of Keith's twitter followers would reach out to Leah and alert her to the tweets. And, as in Example 4, another person might google Leah's name, find the tweets, and let Leah know the tweets exist.

Example 7: Mike creates a Snapchat video threatening Nick. Mike is not friends with Nick or any people who know Nick.

Snapchat is a cell phone application that allows users to post photos and videos within the application. Other users who also have the application can view the videos and photos of people from their phone contact list. No one can view a user's photo or video without the user having the viewer's phone number. All photos and videos are available at most for 24 hours from the time

of posting. Each photo or video may be viewed multiple times within the allotted time period.

The Snapchat video should not count as communication. First, Nick would be very unlikely to see the video himself. Because Snapchat users are friends through cell phone numbers, the only people that would have access to the Snapchat video would be Mike's close friends who have his cell phone number. Additionally, Snapchat videos expire and are inaccessible after 24 hours. This further decreases the likelihood that Nick will find out about the video. Thus, this should not count as communication. Indeed, even if Nick did *in fact* find out about the video through some unusual set of circumstances, Mike did not disregard a reasonable likelihood that he would do so, and thus the test for communication is not satisfied.

CONCLUSION

New technology creates new ways of interacting and requires a more robust definition of communication. Here, we have established a definition of communication that addresses existing means of online interaction and can adapt to new ones. Incorporating this definition of communication into statutes criminalizing cyberharassment will improve the efficacy of those statutes at detecting and punishing problematic online behavior that rises to a level that society deems worthy of criminal sanction.