

A BALANCE OF CONVENIENCE: THE USE OF BURDEN-SHIFTING DEVICES IN CRIMINAL CYBERHARASSMENT LAW

Abstract: As communication using the Internet and electronic media becomes more prevalent, incidents of online harassment have likewise increased. In recent years, the U.S. Congress and state legislatures have enacted new legislation and amended existing criminal statutes to target cyberharassment, also called cyberstalking or cyberbullying. The definition of cyberharassment consequently varies between jurisdictions, particularly with regard to statutory emphasis on the mental state of the accused and the reaction of the victim. This Note argues that the reasonableness and specific intent standards employed by most cyberharassment laws are inadequate to balance the safety interests of victims and the First and Fourteenth Amendment rights of electronic speakers. The Note proposes that cyberharassment statutes be supplemented with burden-shifting devices such as affirmative defenses and nonmandatory presumptions, which have historically been employed in other contexts where the prosecution is procedurally disadvantaged and the details of the crime are peculiarly within the knowledge of the accused. After surveying statutes that have successfully incorporated burden-shifting elements, the Note concludes that reallocating evidentiary burdens increases the efficiency and fairness of cyberharassment law while reconciling the interests of both the victim and the accused.

INTRODUCTION

“I’m your worst nightmare. Your troubles are just beginning.”¹

In May 1998, Taryn Pream, a young woman in Thief River Falls, Minnesota, received this message, accompanied by pornographic pictures, in a series of threatening e-mails sent over a period of three weeks from an anonymous address.² For Pream and law enforcement officials, stopping the online harassment seemed unlikely.³ She had no way of identifying the sender, who appeared to have intimate knowledge of her personal life, and her Internet Service Provider (ISP) could only inform

¹ Naomi Harlin Goodno, *Cyberstalking, A New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 MO. L. REV. 125, 125 (2007) (internal quotation marks omitted).

² Jaime DeLage, *Shut the Door TRF Girl Starts Internet Safety Guide*, GRAND FORKS HERALD, Jan. 26, 1999, at A1.

³ See *id.*

her that the messages originated from her hometown.⁴ Any other information would require at least two weeks and a search warrant.⁵ Pream grew reclusive and paranoid, obsessing about locking doors and windows.⁶ She ultimately tracked down the culprit, not with the assistance of police, but because the sender forwarded several obscene photographs through his friends' e-mail accounts.⁷ One of these individuals helped Pream identify her harasser—a fellow classmate at school.⁸

At the time of Pream's ordeal, her efforts to locate the guilty party were impeded by local authorities' inexperience with the Internet and harassment committed via electronic media.⁹ Federal and state law has progressed significantly since 1998, with over forty states enacting statutes that criminalize cyberbullying, cyberstalking, cyberharassment, and other purposeful, threatening online conduct.¹⁰ Victims of harassment through electronic communications still lack legal remedies, however.¹¹ The U.S. Congress and state legislatures have attempted to address the interests of victims through enacting new legislation or amending existing stalking and harassment laws; yet criminal statutes that contain prosecution-oriented language or subjective standards of harm risk invalida-

⁴ See *id.*

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

⁸ See DeLage, *supra* note 2.

⁹ See *id.* (describing Pream's efforts to stop the harassment by notifying the local sheriff, who admitted he had never used the Internet before).

¹⁰ See *infra* Appendix.

¹¹ See Goodno, *supra* note 1, at 140–41. In recent years there have been several widely publicized teenage suicides as the result of verbal, physical, and electronic harassment. See, e.g., Erik Eckholm & Katie Zezima, *6 Teenagers Are Charged After Classmate's Suicide*, N.Y. TIMES, Mar. 29, 2010, at A1; Christopher Maag, *A Hoax Turned Fatal Draws Anger but No Charges*, N.Y. TIMES, Nov. 28, 2007, at A23. On the rare occasions that these cases have resulted in criminal charges—typically under conventional harassment laws, rather than dedicated cyberharassment statutes—ensuing prosecutions have generally been unsuccessful. For example, in 2006, thirteen-year-old Megan Meier committed suicide after she was harassed on MySpace by a neighborhood mother named Lori Drew, who befriended and then attacked Meier while posing as a sixteen-year-old boy. Maag, *supra*. Drew was charged with criminal violations of the Computer Fraud and Abuse Act (CFAA), but was ultimately acquitted by the U.S. District Court for the Central District of California in 2009. See *United States v. Drew*, 259 F.R.D. 449, 468 (C.D. Cal 2009). More recently, fifteen-year-old Phoebe Prince took her own life after months of online and physical bullying by classmates in South Hadley, Massachusetts. Eckholm & Zezima, *supra*. Although Prince's death has motivated the Massachusetts legislature to enact a new state anti-bullying law and felony charges have been filed against her alleged harassers, some legal experts believe that the criminal charges are too harsh for high school students and will likely be reduced or dismissed. Erik Eckholm & Katie Zezima, *Strategies Take Shape for Trials in Bully Case*, N.Y. TIMES, Sept. 16, 2010, at A19.

tion for impinging on First and Fourteenth Amendment freedoms.¹² Conversely, statutes that feature conservative requirements for conviction impose overwhelming evidentiary burdens upon prosecutors and permit the harasser to continue his or her harmful conduct at the expense of the victim's psychological and even physical well-being.¹³ Identifying an appropriate balance between the interests of both the victim and the accused is therefore essential to ensuring the efficacy and constitutionality of current and future cyberharassment legislation.¹⁴

This Note examines the statutory strategies employed in federal and state cyberharassment laws and proposes that burden-shifting devices, already well established in other areas of penal law, have unique utility for cybercrimes, where anonymous or pseudonymous communications disadvantage victims and law enforcement.¹⁵ Part I explores the nature and consequences of the offense of cyberharassment and how civil immunity for ISPs disincentivizes their disclosure of subscriber identities, even those belonging to individuals who promulgate obscene or objectionable content.¹⁶ Part II examines existing criminal cyberharassment laws and discusses why commonly used statutory elements, such as standards of reasonableness and specific intent, fail to strike an adequate balance between the privacy concerns and personal safety of the victim, and the free speech and due process rights of the alleged harasser.¹⁷ Part III then analyzes the utilitarian benefits, constitutional arguments, and underlying policies of burden-shifting devices, particularly affirmative defenses and nonmandatory presumptions.¹⁸ This Part then proposes that reallocation of evidentiary burdens between the prosecution and the defendant in cyberharassment legislation is a promising method of reconciling the interests of both the victim and the accused.¹⁹ Finally, the Appendix includes all current state and federal cyberharassment statutes, their constituent elements, and the result of any constitutional challenges.²⁰

¹² See Goodno, *supra* note 1, at 141, 144; Eugene Volokh, *Freedom of Speech in Cyberspace from the Listener's Perspective: Private Speech Restrictions, Libel, State Action, Harassment, and Sex*, 1996 U. CHI. LEGAL F. 377, 421.

¹³ See Goodno, *supra* note 1, at 135–36, 138, 143; Joseph C. Merschman, Note, *The Dark Side of the Web: Cyberstalking and the Need for Contemporary Legislation*, 24 HARV. WOMEN'S L.J. 255, 269 (2001).

¹⁴ See Goodno, *supra* note 1, at 133–34, 139.

¹⁵ See *infra* notes 88–257 and accompanying text.

¹⁶ See *infra* notes 21–68 and accompanying text.

¹⁷ See *infra* notes 69–126 and accompanying text.

¹⁸ See *infra* notes 127–164 and accompanying text.

¹⁹ See *infra* notes 165–257 and accompanying text.

²⁰ See *infra* Appendix.

I. THE CRIME OF CYBERHARASSMENT

A. *The Consequences and Legal Difficulties of Cyberharassment*

The terms “cyberharassment,” “cyberbullying,” and “cyberstalking” have no universally accepted definition and are often used interchangeably.²¹ Legal scholars generally distinguish the terms by demographics: cyberbullying²² entails the victimization of minors by other minors, whereas cyberstalking²³ and cyberharassment involve harassment between adults.²⁴ Nevertheless, all three offenses involve un-

²¹ See Goodno, *supra* note 1, at 126.

²² Darby Dickerson, *Cyberbullies on Campus*, 37 U. TOL. L. REV. 51, 56 (2005) (citing CYBERBULLYING.CA, <http://www.cyberbullying.ca> (last visited Jan. 21, 2011)). Cyberbullying refers to the “use of information and communication technologies such as e-mail, cell phone and pager text messages, instant messaging, defamatory personal Web sites, and defamatory online personal polling Web sites, to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others.” *Id.* Studies have shown that cyberbullying tends to peak in middle school and decline in high school, with roughly twenty-five percent of students engaging in or being victimized by some form of Internet harassment. Kirk R. Williams & Nancy G. Guerra, *Prevalence and Predictors of Internet Bullying*, 41 J. ADOLESCENT HEALTH S14, S15, S20 (2007). Notably, prevalence rates of cyberbullying in the United States vary widely between studies, ranging from 6% to as high as 42% of middle and high school students. Jing Wang et al., *School Bullying Among Adolescents in the United States: Physical, Verbal, Relational, and Cyber*, 45 J. ADOLESCENT HEALTH 368, 374 (2009).

Although cyberbullying typically alludes to repetitive, aggressive conduct initiated by children or teenagers towards their peers, by some definitions adults can also engage in cyberbullying towards children or other adults. See Dickerson, *supra*, at 51 (describing incidents of cyberbullying among law students); Andrew M. Hendersen, Note, *High-Tech Words Do Hurt: A Modern Makeover Expands Missouri’s Harassment Law to Include Electronic Communications*, 74 MO. L. REV. 379, 381 (2009) (explaining that although cyberbullying typically involves repetitive, controlling acts by juveniles, adults can also engage in similar behavior). Cyberbullying scholarship frequently focuses on student speech rights on school grounds, the authority of school administrators to regulate that speech, and other civil remedies. See, e.g., Dickerson, *supra*, at 51; Shira Auerbach, Note, *Screening Out Cyberbullies: Remedies for Victims on the Internet Playground*, 30 CARDOZO L. REV. 1641, 1645–47 (2009). Notwithstanding its equal relevance, noncriminal cyberharassment is beyond the scope of this Note, which focuses exclusively on penal statutes. See *infra* Appendix.

²³ U.S. Att’y Gen., *1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry*, U.S. DEP’T OF JUSTICE (Aug. 1999), <http://www.justice.gov/criminal/cybercrime/cyberstalking.htm> [hereinafter *1999 Report on Cyberstalking*]. Cyberstalking involves “the use of the Internet, e-mail, or other electronic communications devices to stalk or harass another person.” *Id.* Cyberstalking is often characterized by repeated predatory behavior or patterns of conduct, which may be accompanied by credible threats of serious harm. Goodno, *supra* note 1, at 126 n.6. The CyberAngels, an anti-cyberstalking nonprofit organization, estimates that at least sixty-three thousand online stalkers currently operate in the United States alone. *Id.* at 156.

²⁴ See Hendersen, *supra* note 22, at 381 (describing cyberbullying as harassment or humiliation of children, preteens, and teenagers); *What Is Cyberbullying, Exactly?*, STOP CYBERBUL-

wanted, repetitious conduct committed through the use of the Internet, cell phone, or other electronic media, with the intent to frighten or harass another person.²⁵ Given their similar characteristics, these terms will be subsumed under the term “cyberharassment” for the purposes of this Note.²⁶

Cyberharassment differs in scope from offline harassment in that the Internet provides an anonymous and relatively unregulated environment where communications can be transmitted instantaneously to a global audience.²⁷ Acts of harassment range from gossip, taunts, and exclusion to explicit sexual harassment, intimidation, or threats.²⁸ Harassers utilize social networking sites like Facebook, MySpace, and LinkedIn, instant messaging, message boards, cell phone text messaging, pagers, and other electronic media to affect their victims over great distances and with minimal effort.²⁹ Technically savvy harassers may use e-mail programs that automatically send messages at regular intervals, overwhelming the victim’s inbox.³⁰

Additionally, harassers can easily obtain the victim’s personal information, such as his or her e-mail address, mailing address, or social security number, and then use this information to intensify their threat-

LYING, http://www.stopcyberbullying.org/what_is_cyberbullying_exactly.html (“Once adults become involved, it is plain and simple cyber-harassment or cyberstalking. Adult cyber-harassment or cyberstalking is NEVER called cyberbullying.”). Cyberbullying and cyberstalking have also been differentiated according to the types of laws that address them, with cyberstalking targeted by stalking laws and cyberbullying by harassment laws. See Hendersen, *supra* note 22, at 381.

²⁵ See Dickerson, *supra* note 22, at 56; Goodno, *supra* note 1, at 126.

²⁶ See 1999 Report on Cyberstalking, *supra* note 23; Dickerson, *supra* note 22, at 56.

²⁷ See Williams & Guerra, *supra* note 22, at S15. The Internet is a particularly popular medium of social interaction for over forty-five million children and teenagers in the United States, who can operate online with more autonomy and less oversight by adults. *Id.*

²⁸ Janis Wolak et al., *Does Online Harassment Constitute Bullying? An Exploration of Online Harassment by Known Peers and Online-Only Contacts*, 41 J. ADOLESCENT HEALTH S51, S51 (2007) (citing J. Patchin & S. Hinduja, *Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying*, 4 YOUTH VIOLENCE & JUV. JUST. 148 (2006)) (subsuming behaviors such as “bothering someone online, teasing in a mean way, calling someone hurtful names, intentionally leaving persons out of things, threatening someone and saying unwanted, sexually related things to someone” under the act of online harassment).

²⁹ See Alison Virginia King, Note, *Constitutionality of Cyberbullying Laws: Keeping the Online Playground Safe for Both Teens and Free Speech*, 63 VAND. L. REV. 845, 850 (2010) (“[A]n Internet-created communication can be widely distributed at the click of a mouse and accessed by not only the bully and target but endless other users as well, particularly if an e-mail is forwarded en masse or if comments are posted on a public website.”).

³⁰ 1999 Report on Cyberstalking, *supra* note 23.

ening conduct,³¹ engage in identity theft,³² or impersonate the victim online.³³ Cyberharassment often involves “stalking by proxy,” where harassers post offensive or inflammatory messages under the victim’s name on bulletin boards or in chatrooms, solicit sexual encounters while posing as the victim on adult personals sites, or otherwise deceive third parties into directing threatening or harassing conduct towards the victim.³⁴ Like physical stalking, online harassment may lead to more dangerous behavior, including physical violence.³⁵ Furthermore, the impersonal nature of electronic communications tends to empower perpetrators who might not otherwise confront the victim in person or over the telephone and enables them to avoid accountability.³⁶

Cyberharassment inflicts significant psychological harm on victims.³⁷ The anonymous or pseudonymous nature of most electronic communications worsens these effects because victims can never be certain that they are safe from attack.³⁸ Unlike traditional stalking or harassment, cyberharassment can reach the victim at any time and follow them anywhere, including into the home, a traditionally private place.³⁹ Cyberharassers can preserve their anonymity with relative ease

³¹ See *id.* (discussing California law enforcement cases in which victims repeatedly received the message “187” on their pagers, alluding to the murder statute of the California Penal Code).

³² See Brian Krebs, *Hackers’ Latest Target: Social Networking Sites*, WASH. POST, Aug. 9, 2008, at A1. (noting that social networking sites have recently become the target of hackers and identity thieves, who hijack accounts or trick users into installing malicious software).

³³ See *1999 Report on Cyberstalking*, *supra* note 23. Certain websites directly assist cyberharassers by supplying instructions regarding how to stalk someone or research a social security number, home address, or driver’s license number. Amy C. Radosevich, Note, *Thwarting the Stalker: Are Anti-Stalking Measures Keeping Pace with Today’s Stalker?*, 2000 U. ILL. L. REV. 1371, 1388.

³⁴ Tom Zeller, Jr., *A Sinister Web Entraps Victims of Cyberstalkers*, N.Y. TIMES, Apr. 17, 2006, at A1. This behavior was illustrated in the case of Gary S. Dellapenta, a Los Angeles security guard who posted rape fantasies in chat rooms and on personals sites under his ex-girlfriend’s name, along with her home address. *Id.* Six different men appeared at the victim’s apartment in response to the advertisements. *Id.* Dellapenta was convicted under California’s cyberstalking law in 1999. *Id.*

³⁵ *1999 Report on Cyberstalking*, *supra* note 23.

³⁶ See *id.*

³⁷ Wang et al., *supra* note 22, at 369; King, *supra* note 29, at 851 (listing low self-esteem, anxiety, alienation, and suicidal tendencies as possible side effects of online harassment).

³⁸ See Goodno, *supra* note 1, at 138 (“[T]he victim may not even know where an anonymous cyberstalker is physically located. For all she knows the cyberstalker may be next door, at her workplace, or across the country . . .”).

³⁹ See Kevin Turbert, Note, *Faceless Bullies: Legislative and Judicial Responses to Cyberbullying*, 33 SETON HALL LEGIS. J. 651, 654 (2009) (“[C]yberbullying has no distinct boundaries and can reach a victim anytime and anywhere.”); see also *Rowan v. U.S. Post Office Dep’t*, 397 U.S. 728, 737 (1970) (holding that the First Amendment does not force individuals to

by using different ISPs, supplying ISPs with incorrect identification information, paying for online services with non-traceable payment methods, or using several different pseudonyms.⁴⁰ When sending e-mail messages, harassers can utilize electronic mail servers that strip away identifying information and transport headers.⁴¹ By forwarding their messages through several such services, they can render their communications untraceable.⁴² Consequently, one of the primary hurdles for cyberharassment victims and government prosecutors is identifying and locating the defendant behind the screen name.⁴³

B. *Subscriber Anonymity and ISP Civil Immunity Under the Communications Decency Act*

In the context of the Internet, anonymous communication is both powerful and prevalent.⁴⁴ In 1995, in *McIntyre v. Ohio Elections Commission*, the U.S. Supreme Court held that “[a]nonymity is a shield from the tyranny of the majority.”⁴⁵ Anonymous communication is protected by the Bill of Rights, particularly the First Amendment, for its ability to foster robust and uninhibited discourse without fear of retaliation or suppression by others.⁴⁶ There is also no doubt that anonymous speech on the Internet receives the same protection under the First Amendment as speech in traditional public fora.⁴⁷ Unfortunately, cyberharass-

experience unwanted communication in the privacy of the home); Wolak et al., *supra* note 28, at S52 (“[T]he nature of the Internet creates the potential for repeated victimization, and when harassment is posted online, it may not be easy for a target to terminate the situation.”).

⁴⁰ 1999 Report on Cyberstalking, *supra* note 23.

⁴¹ *Id.*

⁴² *Id.*

⁴³ *See id.*

⁴⁴ *See* Dickerson, *supra* note 22, at 56; Goodno, *supra* note 1, at 130–31.

⁴⁵ 514 U.S. 334, 357 (1995).

⁴⁶ *See id.* In *McIntyre*, the U.S. Supreme Court struck down an Ohio statute that required political handbills to identify the author or organization responsible for writing or distributing them, holding:

Whatever the motivation may be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author’s decision to remain anonymous . . . is an aspect of the freedom of speech protected by the First Amendment.

Id. at 341–42.

⁴⁷ *See* *Reno v. ACLU*, 521 U.S. 844, 870 (1997) (“As the District Court found, ‘the content on the Internet is as diverse as human thought.’ We agree with its conclusion that our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium.”); Matthew Mazzotta, Note, *Balancing Act: Finding Consensus on*

ers frequently take advantage of their anonymity to conceal their true identities and locations, inflict additional psychological harm on victims, and impair attempts at legal prosecution.⁴⁸ In order for the government to identify and successfully prosecute these offenders, prosecutors must first obtain their identification information from ISPs.⁴⁹

ISPs that host e-mail services, social websites, and bulletin boards often serve as the “first line of defense” against cyberharassment, providing filtering options that allow users to block unwanted or unfamiliar e-mails, instant messages, or postings to their online profiles.⁵⁰ ISPs typically have policies that prohibit the abuse of their services, and they typically retain the right to terminate a user’s account if he or she violates these policies.⁵¹ When cyberharassment escalates beyond these initial protective measures, ISPs can also identify specific users and their locations based on their Internet Protocol (IP) addresses and remove objectionable content at the request of petitioning parties.⁵² ISPs have no legal obligation to comply with such requests, however, and frequently ignore them, claiming that implementing additional customer protection would be costly and inefficient.⁵³ Unlike copyright law, where federal statutory authority provides a subpoena power that forces ISPs to disclose user information outside the discovery process,⁵⁴ ISP liability in the context of cyberharassment is dictated by the Federal Communications Decency Act (CDA).⁵⁵

Standards for Unmasking Anonymous Internet Speakers, 51 B.C. L. REV. 833, 839 (2010) (“Speech on the internet receives full First Amendment protection, including the right to speak anonymously.”).

⁴⁸ See 1999 Report on Cyberstalking, *supra* note 23.

⁴⁹ See *id.*

⁵⁰ Merschman, *supra* note 13, at 277.

⁵¹ *Id.*; see Jennifer Steinhauer, *Woman Indicted in MySpace Suicide Case*, N.Y. TIMES, May 16, 2008, at A1 (describing the indictment of Lori Drew under the CFAA, premised upon Drew’s violation of MySpace’s user agreement).

⁵² See Turbert, *supra* note 39, at 678–79. The ability of an ISP to identify subscribers based on their IP addresses depends on whether the subscribers supplied the ISPs with accurate identification information. See Laurence H. Miller et al., *Responding to the Anonymous Cyber-Griper*, ACCA DOCKET, May 2002, at 64, 82 (“There is no guarantee, however, that John Doe gave [the] ISP the correct information. Ultimately, the information that the plaintiff obtains may be worthless.”). Such deception is often overlooked because ISPs rarely authenticate or confirm user data so long as they receive payment for their services in a timely manner. See 1999 Report on Cyberstalking, *supra* note 23.

⁵³ See 1999 Report on Cyberstalking, *supra* note 23. ISPs argue that “no attempt to impose cyberstalking reporting or response requirements should be made unless fully justified” on the grounds that the “decentralized nature of the Internet would make it difficult for providers to collect and submit such data.” *Id.*

⁵⁴ Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512(h) (2006).

⁵⁵ See 47 U.S.C. § 230 (2006).

Prior to the enactment of the CDA, ISPs could be found directly, vicariously, or contributorily liable for defamatory statements posted on their networks, particularly if they exercised any editorial control over user postings.⁵⁶ Only ISPs that acted as a “passive conduit” of information could escape liability.⁵⁷ This rule forced providers to choose between disregarding offensive content entirely in order to maintain their status as a “passive conduit,” or else regulate all content and risk liability for any objectionable message that was overlooked.⁵⁸ Congress enacted § 230 specifically to address this issue.⁵⁹

Section 230 provides two layers of immunity for ISPs.⁶⁰ First, service providers cannot be held liable as speakers, publishers, or distributors of obscene, harassing, or otherwise objectionable content posted by users.⁶¹ Even if the ISP possesses the ability to publish, withdraw, or

⁵⁶ See *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710, at *1, *5–6 (N.Y. Sup. Ct. 1995) (holding ISP defendant liable for defamatory postings on a message board because the ISP exercised editorial control and judgment over user messages by implementing an automatic scanning process).

⁵⁷ See *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135, 140 (S.D.N.Y. 1991) (finding defendant ISP was not directly or vicariously liable for defamatory statements posted on its bulletin board because the ISP exercised little editorial control over the content of its forums or its third party users); *Stratton Oakmont Inc.*, 1995 WL 323710, at *3 (“A distributor or deliverer of defamatory material is considered a passive conduit and will not be found liable in the absence of fault.”).

⁵⁸ See *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997) (explaining that Congress enacted § 230 to remove ISP disincentives for self-regulation or blocking of offensive material, as introduced by the *Stratton Oakmont* decision); Lisa Guernsey, *Telling Tales out of School*, N.Y. TIMES, May 8, 2003, at G1 (“As long as Web hosting companies and other providers make no attempt to edit what shows up [on] their sites, they cannot be sued for what appears on them.”).

⁵⁹ See *Zeran*, 129 F.3d at 331.

⁶⁰ See 47 U.S.C. § 230(c). Section 230(c) of the CDA provides:

(1) Treatment of publisher or speaker. No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability. No provider or user of an interactive computer service shall be held liable on account of—(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not, such material is constitutionally protected; or (B) any action to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

Id. § 230(c)(1)–(2).

⁶¹ See *id.* § 230(c)(1). The CDA does not extend ISP immunity to criminal liability. Joanna Lee Mishler, Comment, *Cyberstalking: Can Communication via the Internet Constitute a Credible Threat and Should an Internet Service Provider Be Liable if It Does?*, 17 SANTA CLARA COMPUTER & HIGH TECH. L.J. 115, 131 (2000).

change content on its servers and has knowledge that users have engaged in defamatory or slanderous speech, it cannot be held liable for content-based claims under § 230.⁶² This aspect of immunity protects ISPs from all civil claims, including tort and breach of contract claims, and typically applies in cases involving defamation, negligence, libel, and slander.⁶³ Second, § 230 protects ISPs in their good faith efforts to restrict user access to objectionable content, regardless of whether that content is normally protected by the First Amendment.⁶⁴

In cases where an ISP refuses to voluntarily reveal the identity of an anonymous or pseudonymous subscriber, in the civil context, a cyber-harassment victim has no option other than to file a “John Doe” lawsuit and attempt to compel ISP disclosure through discovery.⁶⁵ Nevertheless, even a victorious “John Doe” suit may not reveal the culprit’s identity if the subscriber originally supplied the ISP with false information or the ISP already deleted its relevant access logs.⁶⁶ Although courts have recognized the importance of anonymous speech with regard to books, pamphlets, handbills, and other printed publications, they have found a more limited privacy interest in anonymous Internet postings, and must balance the defendant’s First Amendment right to speak anonymously against the right of the plaintiff to protect his or her proprietary interests and reputation.⁶⁷ Revealing anonymous speakers may chill legiti-

⁶² See *Zeran*, 129 F.3d at 330.

⁶³ See, e.g., *id.* at 330–31 (determining an ISP to be immune from charges of defamation and harassment); *Shneider v. Amazon.com, Inc.*, 31 P.3d 37, 42 (Wash. Ct App. 2001) (acknowledging that courts analyzing the scope of § 230 have found the statute provides immunity to civil claims generally).

⁶⁴ See 47 U.S.C. § 230(c) (2).

⁶⁵ See *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999); *Mazzotta*, *supra* note 47, at 834. In *Columbia Insurance Co.*, a trademark infringement case, the U.S. District Court for the Northern District of California provided criteria for the discovery of a defendant’s identity from an ISP, explaining that:

With the rise of the Internet has come the ability to commit certain tortious acts . . . entirely on-line. The tortfeasor can act pseudonymously or anonymously and may give fictitious or incomplete identifying information. Parties who have been injured by these acts are likely to find themselves chasing the tortfeasor from Internet Service Provider (ISP) to ISP, with little or no hope of actually discovering the identity of the tortfeasor.

185 F.R.D. at 578.

⁶⁶ *Miller et al.*, *supra* note 52, at 82. Conversely, in the field of defamation, it has been argued that “unmasking subpoenas” served on ISPs allow plaintiffs to identify anonymous defendants too easily, thereby silencing online speakers and possibly exposing them to intimidation and retaliation. *Mazzotta*, *supra* note 47, at 840, 843.

⁶⁷ See *Dendrite Int’l, Inc. v. Doe No. 3*, 775 A.2d 756, 760–61, 765 (N.J. Super. Ct. App. Div. 2001) (quoting *Talley v. California*, 362 U.S. 60, 64 (1960)) (“Anonymous pamphlets,

mate discourse; at the same time, victims must discover defendants' identities in order to have the opportunity to pursue legal relief.⁶⁸

II. FEDERAL AND STATE LEGISLATIVE APPROACHES TO CYBERHARASSMENT

A. *What Controls: The Perspective of the Victim or of the Harasser?*

Although forty-six states now include electronic communications in their stalking and harassment laws, the status of American cyberharassment law remains inconsistent.⁶⁹ State statutes feature differing causes of action, requisite mental states, and punishments.⁷⁰ At the federal level, there are three federal statutes that can be applied to cyberharassment: the Interstate Communications Act,⁷¹ the Interstate Stalking Punishment and Prevention Act (the "Interstate Stalking Act"),⁷²

leaflets, brochures and even books have played an important role in the progress of mankind."). The Superior Court of New Jersey articulated a four-step test for trial courts contemplating an order to compel an ISP to disclose the identity of an anonymous Internet subscriber: (1) efforts by the plaintiff to notify anonymous posters that they are the subject of a subpoena or order for disclosure; (2) identification by the plaintiff of the exact statements made by each anonymous poster that constitute actionable speech; (3) review of the complaint and all information provided to the court to determine whether the plaintiff has established a prima facie cause of action against the anonymous defendants; and (4) balancing the defendant's right of free speech and the necessity of disclosure of the defendant's identity. *Id.* at 760–61. The *Dendrite* analysis, although influential, is but one of several balancing tests employed at the state and federal levels. Mazzotta, *supra* note 47, at 846.

⁶⁸ Miller et al., *supra* note 52, at 77; Mazzotta, *supra* note 47, at 834–35.

⁶⁹ See Goodno, *supra* note 1, at 142; *State Cyberstalking, Cyberharassment and Cyberbullying Laws*, NAT'L CONF. ST. LEGISLATURES, <http://www.ncls.org/IssuesResearch/TelecommunicationsInformationTechnology/CyberstalkingLaws/tabid/13495/Default.aspx> (last updated Dec. 20, 2010). States that have enacted cyberharassment legislation have primarily done so by amending existing stalking or harassment laws or expanding their definition of stalking or harassment to include electronic means of communication. Shonah Jefferson & Richard Shafritz, *A Survey of Cyberstalking Legislation*, 32 UWLA L. REV. 323, 329 (2001). A few states, including Arkansas, Virginia, and Wisconsin, have also introduced new statutes specifically targeting unlawful electronic communications. *Id.* at 330.

⁷⁰ See Goodno, *supra* note 1, at 142.

⁷¹ 18 U.S.C. § 875(c) (2006). The Interstate Communications Act criminalizes any communication that is transmitted in interstate commerce and contains a threat to injure the person of another, which includes communications through telephone, beepers, or the Internet. See Goodno, *supra* note 1, at 148. In 1999, the U.S. Court of Appeals for the Tenth Circuit upheld a conviction under § 875(c) where the defendant sent a bomb threat to his girlfriend using AOL's instant messenger service. See *United States v. Kammerzell*, 196 F.3d 1137, 1138, 1139 (1999).

⁷² 18 U.S.C. § 2261A (2006). At the time of its enactment in 1996, the Interstate Stalking Act constituted the first federal law to specifically address physical stalking. Goodno, *supra* note 1, at 151, 152. In 2000, Congress amended the statute for the first time via the

and the CDA.⁷³ These federal laws have their own limitations because they were originally designed to prohibit physical stalking, obscenity, or child pornography rather than cyberharassment.⁷⁴ Additionally, all cyberharassment statutes remain vulnerable to constitutional challenges for substantial overbreadth or vagueness due to their potential restrictions on protected speech.⁷⁵

Victims of Trafficking and Violence Protection Act of 2000 (the “Victims of Trafficking Act”), which changed the statute’s language to target defendants who travel in interstate or foreign commerce, regardless of whether the defendant physically moves across state lines. *See id.* at 151. Although the Victims of Trafficking Act did not address whether a person could travel in interstate commerce via the Internet, in 2004, the U.S. Court of Appeals for the Sixth Circuit found a defendant guilty of cyberstalking under § 2261A. *See United States v. Bowker*, 372 F.2d 365, 388 (6th Cir. 2004); Goodno, *supra* note 1, at 151.

In January 2006, the Interstate Stalking Act was amended a second time by the Violence against Women and Department of Justice Reauthorization Act of 2005 (VAWA), Pub. L. No. 109-162, § 114, 119 Stat. 2960, 2987. *See* Goodno, *supra* note 1, at 152. Section 2261A was expanded to criminalize any course of conduct that causes substantial emotional distress through the defendant’s use of an interactive computer service. *See id.*

⁷³ 47 U.S.C. § 223 (2006). The CDA originated from the Communications Act of 1934, which was subsequently amended by the Telecommunications Act of 1996, Pub. L. No. 104-104, § 1, 110 Stat. 56, 133 (codified as amended at 47 U.S.C. § 223). Congress incorporated the CDA in title V, section 502 of the Telecommunications Act. *See* Telecommunications Act § 502. In January 2006, Congress amended the CDA when it enacted VAWA, which modified the definition of the term “telecommunications” to include “any device or software that can be used to originate telecommunications or other types of communications that are transmitted, in whole or in part, by the Internet.” *See* 47 U.S.C. § 223(h)(1)(C).

⁷⁴ *See* King, *supra* note 29, at 856 (describing the shortcomings of these statutes). For example, the Interstate Communications Act is arguably of limited use in cyberharassment cases because the statute only applies to overt threats, excluding cases where the cyberharasser indirectly interacts with the victim or causes psychological, rather than bodily, harm. *See id.*

⁷⁵ *See* *Reno v. ACLU*, 521 U.S. 844, 858 (1997). The overbreadth doctrine mandates that a statute be struck down if its scope encompasses free expression protected by the First Amendment in addition to legitimately forbidden conduct. *See, e.g., Thornhill v. Alabama*, 310 U.S. 88, 97 (1940) (“A [] threat is inherent in a penal statute . . . which does not aim specifically at evils within the allowable area of state control but, on the contrary, sweeps within its ambit other activities that in ordinary circumstances constitute an exercise of freedom of speech or of the press.”). The void-for-vagueness doctrine raises due process considerations where statutory language is so ambiguously drafted that it fails to provide fair warning for potential defendants and encourages arbitrary enforcement. *See* Merschman, *supra* note 13, at 273. Notably, legislatures can criminalize true threats—serious statements that express intent to commit an act of unlawful violence—because threats do not fall within the protection of the First Amendment. *See* *Virginia v. Black*, 538 U.S. 343, 344 (2003) (ruling that the First Amendment permits states to ban true threats); *Watts v. United States*, 394 U.S. 705, 707 (1969) (per curiam) (holding that true threats, despite being a form of pure speech, should be distinguished from constitutionally protected speech).

The CDA has been successfully challenged on the constitutional grounds of substantial overbreadth. *See* *Reno v. ACLU*, 521 U.S. at 882–83. In *Reno v. ACLU*, the U.S. Supreme Court struck down the CDA’s prohibition on “indecent” and “patently offensive” communications transmitted over the Internet to minor recipients as being facially unconstitutional. *Id.* Nev-

This patchwork of federal and state law generates substantial technical disparities between jurisdictions, particularly with regard to statutes' varying emphases on the perspectives of the victim and alleged harasser.⁷⁶ Some legal scholarship suggests that cyberharassment should be based on the perception of the victim.⁷⁷ To illustrate this concept, two scholars pose the hypothetical of a secret admirer who sends flowers to a girl to demonstrate his romantic interest.⁷⁸ If the girl does not respond, but nevertheless receives more flowers from her admirer on the following day, does this constitute harassment?⁷⁹ Even though an objective observer might consider this culpable behavior, if the victim is not upset by the suitor's attention, then arguably, no crime has been committed.⁸⁰

Other commentators counter that measuring the defendant's culpability according to the subjective effect on the victim conflicts with First Amendment principles, particularly when a statute regulates speech in addition to conduct.⁸¹ In the absence of an objective standard, a statute may provide insufficient notice to ordinary citizens of what conduct is prohibited, particularly when the law utilizes general terms like "annoying," "harassing," and "indecent."⁸² Such statutes potentially could be struck down for being unconstitutionally vague.⁸³ A

ertheless, in order to preserve the remainder of the statute, the Court severed the indecency provision while preserving the government's right to prosecute obscenity and child pornography. *Id.* at 883.

⁷⁶ See Goodno, *supra* note 1, at 140–41.

⁷⁷ See Diana Lamplugh & Paul Infield, *Harmonising Anti-Stalking Laws*, 34 GEO. WASH. INT'L L. REV. 853, 868 (2003).

⁷⁸ See *id.*

⁷⁹ See *id.*

⁸⁰ See *id.*

⁸¹ See Gene Barton, Note, *Taking a Byte out of Crime: E-mail Harassment and the Inefficacy of Existing Law*, 70 WASH. L. REV. 465, 481–82 (1995) (using the constitutionality of telephone harassment statutes as guidance for e-mail harassment laws).

⁸² See Volokh, *supra* note 12, at 421.

⁸³ See *State v. Bryan*, 910 P.2d 212, 220 (Kan. 1996); Volokh, *supra* note 12, at 421. In the 1996 case of *State v. Bryan*, the Kansas Supreme Court struck down a state stalking law as being unconstitutionally vague, explaining:

The danger in this situation is obvious. In the absence of an objective standard, the terms "annoys," "alarms" and "harasses" subject the defendant to the particular sensibilities of the individual victim. Different persons have different sensibilities, and conduct which annoys or alarms one person may not annoy or alarm another. The victim may be of such a state of mind that conduct which would never annoy, alarm, or harass a reasonable person would seriously annoy, alarm, or harass this victim. In such a case, the defendant would be guilty of stalking . . . even though a reasonable person in the same

subjective, victim-based standard also disregards the reality that rude, provocative, and offensive statements are considered common Internet parlance and do not distress most users.⁸⁴ Such statements can occur spontaneously, without menacing intent, and are considered constitutionally protected speech.⁸⁵

Legislators seeking to define the offense of cyberharassment must balance the First Amendment interests of electronic speakers with the protection of victims from genuinely harmful and threatening conduct.⁸⁶ Consequently, federal and state legislatures have adopted certain mechanisms to reconcile the interests of the victim and alleged harasser: (1) an objective or subjective reasonable person test based on the victim's perspective, (2) an objective reasonable person test based on the harasser's perspective, (3) a specific intent element, or (4) some combination of the above.⁸⁷

B. *Statutory Schemes Involving Elements of Reasonableness or Specific Intent*

1. Reasonableness Standard Based on the Victim

Several state statutes use an objective "reasonable victim" standard, which requires the factfinder to determine whether the defendant's actions would have caused a reasonable person to suffer serious inconvenience, emotional distress, or fear of bodily injury to themselves or their family members.⁸⁸

situation would not be alarmed, annoyed, or harassed by the defendant's conduct.

910 P.2d at 220.

⁸⁴ See Wolak et al., *supra* note 28, at S52, S57. In one study involving ten- and seventeen-year-olds, the majority of online harassment incidents were not found to be distressing. *Id.* at S57. Subjects who visited chatrooms regularly or used the Internet while visiting friends' houses were less likely to be threatened by online harassment, possibly because they had become inured to online incivility or felt more secure because of their offline social situation. *Id.*

⁸⁵ See Volokh, *supra* note 12, at 422–23 ("This sort of conduct seems less like a deliberately harassing phone call, and more like the annoying words said in public . . . which are generally not punishable unless they're likely to cause a fight.")

⁸⁶ See Goodno, *supra* note 1, at 133–34, 139.

⁸⁷ See *infra* Appendix. Additionally, more than twenty state criminal laws exempt constitutionally protected activities, such as organized protests, from their purview. See, e.g., FLA. STAT. ANN. § 817.568 (West 2006); LA. REV. STAT. ANN. § 14:40.2 (West, Westlaw through 2007 Sess.); R.I. GEN. LAWS § 11-52-4.2 (West, Westlaw through 2008 Sess.). These statutes are also noted in the Appendix. See *infra* Appendix.

⁸⁸ See N.J. STAT. ANN. 2C:12-10(b) (West 2005 & Supp. 2010) ("A person is guilty of stalking, a crime in the fourth degree, if he purposefully or knowingly engages in a course of conduct directed at a specific person that would cause a reasonable person to fear for

Some scholars criticize this statutory element on the grounds that an objective standard discounts the victim's personal reaction to the defendant's conduct and does not allow the court sufficient flexibility to evaluate incidents of cyberharassment on a case-by-case basis.⁸⁹ Cyberharassers seldom make overt threats and often act indirectly, such as by inducing third parties to harass the victim for them.⁹⁰ Additionally, many Internet users are accustomed to some measure of unpleasant online behavior.⁹¹ Depending on the circumstances, conduct that may seem innocuous to the judicial factfinder may make a particular victim feel genuinely frightened, in a way that arguably deserves some remedy at law.⁹² In response to this concern, states such as Arizona, Oklahoma, and Nevada supplement their objective "reasonable victim" standard with an additional subjective element that requires that the harassing conduct actually cause the victim to feel fear, alarm, or emotional distress.⁹³

Conversely, a subjective reasonableness standard that relies on the victim's unique perception of the defendant's conduct, although taking account of the victim's individual circumstances, could expand the offense to the point of overbreadth.⁹⁴ In fact, state statutes that have at-

his safety or the safety of a third person or suffer emotional distress."); OKLA. STAT. ANN. tit. 21, § 1173(A)(1) (2002) ("Any person who . . . [w]ould cause a reasonable person or a member of the immediate family of that person . . . to feel frightened, intimidated, threatened, harassed, or molested . . .").

⁸⁹ See Lamplugh & Infield, *supra* note 77, at 868 ("Stalking is . . . a crime that depends on perception, particularly that of the victim."); Radosevich, *supra* note 33, at 1384.

⁹⁰ See Zeller, *supra* note 34.

⁹¹ See Wolak et al., *supra* note 28, at S52, S57.

⁹² See Radosevich, *supra* note 33, at 1384.

⁹³ See ARIZ. REV. STAT. ANN. § 13-2921 (2010) (defining "harassment" as conduct "that would cause a reasonable person to be seriously alarmed, annoyed or harassed and the conduct in fact seriously alarms, annoys or harasses the person"); NEV. REV. STAT. ANN. § 200.575 (LexisNexis 2006 & Supp. 2009) (requiring that the defendant's conduct "actually causes the victim to feel terrorized, frightened, intimidated or harassed"); OKLA. STAT. ANN. tit. 21, § 1173(A)(2) (targeting any defendant who "[a]ctually causes the person being followed or harassed to feel terrorized, frightened, intimidated, threatened, harassed, or molested"); see also *Cyberbullying and Other Online Safety Issues for Children: Hearing on H.R. 1966, the "Megan Meier Cyberbullying Prevention Act" and H.R. 3630, the "Adolescent Web Awareness Requires Education Act (AWARE Act)" Before the H. Judiciary Subcomm. on Crime, Terrorism, and Homeland Sec.*, 111th Cong. 39 (2009) [hereinafter *Hearing on Megan Meier Cyberbullying Prevention Act and AWARE Act*] (statement by Robert M. O'Neil, Director of the Thomas Jefferson Center for the Protection of Free Expression) (proposing that a specific intent element, as well as required proof of impact or harm upon the victim, enhances the efficacy of criminal cyberbullying statutes).

⁹⁴ See Lamplugh & Infield, *supra* note 77, at 865 (acknowledging that the United Kingdom's Prevention of Harassment Act, 1997, 25 & 26 Eliz. 2, c. 40 (Eng.), which defines

tempted to define cyberharassment entirely in terms of the victim's personal reaction have been invalidated on the grounds that overly subjective standards may lead to unconstitutional vagueness.⁹⁵ Although a cause of action should be available for victims who have suffered actual harm attributable to cyberharassment, legislatures that have chosen an objective "reasonable victim" standard likely sought to limit lawsuits by exceptionally sensitive individuals.⁹⁶ Furthermore, purely offensive speech or profanity has traditionally been afforded protection by the First Amendment.⁹⁷ In order to silence such speech, there must be a showing that listeners are captive audiences whose privacy interests have been invaded in an intolerable manner, or that the listeners have been subjected to unwanted communications in the sanctuary of the home.⁹⁸ It could be argued that cyberharassment victims could easily "avert their eyes" by turning off the electronic device or simply ignoring the offensive communication.⁹⁹ The fact that most users tolerate ribald online remarks as a matter of course reinforces this point.¹⁰⁰

stalking and harassment according to the victim's perspective, has raised judicial concern regarding its broad scope).

⁹⁵ See *Karenev v. State*, 258 S.W.3d 210, 214, 217 (Tex. App. 2008) (ruling that a provision of Texas's harassment statute, which prohibited the transmission of electronic communications in a manner "reasonably likely to harass, annoy, alarm, abuse, torment, embarrass, or offend," was void for vagueness because the prohibited standard of conduct depended on each complainant's individual sensitivity), *rev'd on other grounds*, 281 S.W.3d 428 (Tex. Crim. App. 2009); *State v. Williams*, 26 P.3d 890, 895 (Wash. 2001) (ruling that part of Washington's harassment law was unconstitutionally vague and overbroad due to the statute's reliance on an inherently subjective standard regarding the effect of the defendant's conduct upon the victim's "mental health"); see also *City of Bellevue v. Lorang*, 992 P.2d 496, 502 (Wash. 2000) ("This court has invalidated criminal laws for vagueness when they are overly subjective.").

⁹⁶ See *Bryan*, 910 P.2d at 220.

⁹⁷ See, e.g., *Cohen v. California*, 403 U.S. 15, 21 (1971) ("[T]he mere presence of unwitting listeners or viewers does not serve automatically to justify curtailing all speech capable of giving offense.").

⁹⁸ See *id.*; *Rowan v. U.S. Post Office Dep't*, 397 U.S. 728, 737 (1970).

⁹⁹ See *Cohen*, 403 U.S. at 21 (determining that individuals in a courthouse could have simply averted their eyes in order to avoid seeing the defendant's offensive message). But see Patrick M. Garry, *The First Amendment and Non-Political Speech: Exploring a Constitutional Model That Focuses on the Existence of Alternative Channels of Communication*, 72 MO. L. REV. 477, 498-99 (2007) (arguing that it is not possible to avert one's eyes from violent or indecent electronic communications because the Internet has become a function of everyday life and users, particularly minors, sitting at computer screens could be considered a captive audience).

¹⁰⁰ See Wolak et al., *supra* note 28, at S57; *supra* note 84 and accompanying text.

2. Reasonableness Standard Based on the Alleged Harasser

Several states, including Minnesota, New Hampshire, Tennessee, and Utah employ an objective “reasonable harasser” standard based on whether the defendant knew or should have reasonably known that his or her actions would cause an individual emotional distress or fear for his or her safety.¹⁰¹

This standard is sometimes preferred over a specific intent element because it provides sufficient notice to the defendant that his or her conduct may be illegal without imposing an overwhelming evidentiary burden on the government.¹⁰² Furthermore, it recognizes that a victim may suffer psychological harm regardless of whether the defendant actually intended to cause that harm.¹⁰³ Minnesota’s harassment and stalking statute explicitly favors an objective “reasonable harasser” approach over specific intent for these reasons.¹⁰⁴

Nevertheless, statutes that feature a “reasonable harasser” standard have been disparaged by legal scholars who believe that harassment laws should focus on the impact on the victim, who is mentally and perhaps physically harmed as the result of the offense, as opposed to the conduct of the harasser.¹⁰⁵ Statutes using this standard also could be subject to First Amendment challenges based on overbreadth.¹⁰⁶ For example, in 2008, the Supreme Court of Oregon in *State v. Johnson* invalidated a provision of Oregon’s harassment statute that criminalized public insults

¹⁰¹ See, e.g., MINN. STAT. ANN. § 609.749 (West 2009) (“[‘Harass’] means to engage in intentional conduct which: (1) the actor knows or has reason to know would cause the victim under the circumstances to feel frightened, threatened, oppressed, persecuted, or intimidated; and (2) causes this reaction on the part of the victim.”); N.H. REV. STAT. ANN. § 633:3-a (2007) (targeting conduct that the actor knows will place an individual in fear for his or her personal safety or the safety of his or her family); TENN. CODE ANN. § 39-17-308 (2010) (prohibiting communication, without legitimate purpose, “[i]n a manner the defendant knows, or reasonably should know, would frighten, intimidate or cause emotional distress to a similarly situated person of reasonable sensibilities”); UTAH CODE ANN. § 76-5-106.5 (LexisNexis 2008) (providing that a person is guilty of stalking where he or she “knows or should know that the course of conduct would cause a reasonable person” to fear for his or her safety or experience emotional distress).

¹⁰² See Merschman, *supra* note 13, at 270.

¹⁰³ See *id.* at 287.

¹⁰⁴ See MINN. STAT. ANN. § 609.749(1a) (“In a prosecution under this section, the state is not required to prove that the actor intended to cause the victim to feel frightened, threatened, oppressed, persecuted, or intimidated . . .”).

¹⁰⁵ See Goodno, *supra* note 1, at 146–47.

¹⁰⁶ See *State v. Johnson*, 191 P.3d 665, 667–69 (Or. 2008) (“Taunts intended and likely to produce a violent response are not limited to playgrounds and gang disputes. They extend to political, social, and economic confrontations . . . and thus include a wide range of protected speech.”).

using “abusive words or gestures in a manner intended and likely to provoke a violent response,” as facially overbroad because the statute could be extended to political disputes and other protected speech.¹⁰⁷

3. Specific Intent

Section 223 of the CDA and several state laws, including Arkansas, Iowa, and Pennsylvania, require the harasser to act with intent to harass, annoy, alarm, abuse, torment, or embarrass the victim.¹⁰⁸ Specific intent is associated with the offense’s mens rea and most often targets “purposeful,” “willful,” or “knowing” behavior.¹⁰⁹ Specific intent is an efficient means of identifying culpable behavior that should be sanctioned in criminal law.¹¹⁰ Statutes containing specific intent elements are also more likely to be considered conduct based rather than purely speech based, and would therefore be more likely to withstand an overbreadth challenge under the First Amendment.¹¹¹

Nonetheless, this element has been criticized because of the heavy burden it places upon the state to show the requisite intent beyond a reasonable doubt.¹¹² Cyberharassers engage in threatening conduct based on any number of motives that can be impossible for the prosecution to identify.¹¹³ This evidentiary requirement is further complicated when the defendant has no previous relationship with the victim or is physically located a great distance away, and therefore seemingly lacks the intent or ability to follow through with threats made online.¹¹⁴

¹⁰⁷ *Id.*

¹⁰⁸ *See, e.g.*, 47 U.S.C. § 223(a)(1)(C) (2006) (“Whoever . . . makes a telephone call or utilizes a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person”); ARK. CODE ANN. § 5-41-108 (2006) (“A person commits the offense of unlawful computerized communications if, with the purpose to frighten, intimidate, threaten, abuse, or harass another person”); IND. CODE ANN. § 35-45-2-2(a)(4) (LexisNexis 2009) (“A person who, with intent to harass, annoy, or alarm another person but with no intent of legitimate communication”); 18 PA. CONS. STAT. ANN. § 2709 (West 2000 & Supp. 2010) (“A person commits the crime of harassment when, with intent to harass, annoy, or alarm another”).

¹⁰⁹ *See* Radosevich, *supra* note 33, at 1385.

¹¹⁰ *See* Jefferson & Shafritz, *supra* note 69, at 338 (“It seems appropriate to address computerized communications that are intended to threaten, harass, intimidate and harm individuals given the widespread use of computers and the Internet.”).

¹¹¹ *See* Barton, *supra* note 81, at 471 n.49, 481.

¹¹² *See* Merschman, *supra* note 13, at 269.

¹¹³ *See* Lamplugh & Infield, *supra* note 77, at 865 (“[A] requirement that the prosecution prove an intent to stalk would emasculate the law because many stalkers harass their victims not out of malevolent intent but from other motives.”).

¹¹⁴ *See* Radosevich, *supra* note 33, at 1384–85.

4. Combination Statutes

The majority of statutes employ a combination of the aforementioned elements, typically combining specific intent and some kind of reasonableness standard.¹¹⁵ It is frequently unclear, however, whether the reasonableness standard is based on the perspective of the victim or the harasser, particularly if the statute merely prohibits conduct that is “likely” to cause harm.¹¹⁶ Some states, such as California and Missouri, merge intent and reasonableness requirements by targeting defendants who act “with intent to place the victim in reasonable fear.”¹¹⁷

¹¹⁵ See, e.g., 18 U.S.C. § 2261A (2006); ALA. CODE ANN. § 13A-11-8 (LexisNexis 2005); CAL. PENAL CODE § 646.9 (West 2010); MICH. COMP. LAWS ANN. § 750.411s (West 2004). One of Michigan’s cyberharassment statutes, which includes an objective and subjective reasonable victim requirement, an objective reasonable harasser requirement, and a specific intent element, provides in relevant part:

(1) A person shall not post a message through the use of any medium of communication, including the internet or a computer, computer program, computer system, or computer network, or other electronic medium of communication, without the victim’s consent, if all of the following apply:

(a) The person knows or has reason to know that posting the message could cause 2 or more separate noncontinuous acts of unconsented contact with the victim.

(b) Posting the message is intended to cause conduct that would make the victim feel terrorized, frightened, intimidated, threatened, harassed, or molested.

(c) Conduct arising from posting the message would cause a reasonable person to suffer emotional distress and to feel terrorized, frightened, intimidated, threatened, harassed, or molested.

(d) Conduct arising from posting the message causes the victim to suffer emotional distress and to feel terrorized, frightened, intimidated, threatened, harassed, or molested.

MICH. COMP. LAWS ANN. § 750.411s(1)(a)–(d).

¹¹⁶ See, e.g., ALA. CODE ANN. § 13A-11-8(b)(1)(a) (“A person commits the crime of harassing communications if, with intent to harm or alarm another person, he or she . . . communicates with a person, anonymously or otherwise . . . in a manner likely to harass or cause alarm.”); CONN. GEN. STAT. ANN. § 53a-182b (West 2007) (“A person is guilty of harassment in the first degree when, with the intent to harass, annoy, alarm or terrorize another person, he . . . communicates such threat . . . in a manner likely to cause annoyance or alarm . . .”); N.Y. PENAL LAW § 240.30(1)(a) (McKinney 2008) (“A person is guilty of aggravated harassment in the second degree when, with intent to harass, annoy, threaten, or alarm another person, he or she . . . communicates with a person, anonymously or otherwise . . . in a manner likely to cause annoyance or alarm . . .”); see also Long v. State, 931 S.W.2d 285, 289, 290 n.4 (Tex. Crim. App. 1996) (stating that the language “reasonably likely,” standing alone, does not indicate an objective reasonableness standard and even if such a standard were present, it could not save a statute from constitutional challenge if the prohibited conduct is too vague or overbroad).

¹¹⁷ See CAL. PENAL CODE § 646.9(a) (“Any person who willfully, maliciously, and repeatedly follows or willfully and maliciously harasses another person and who makes a

Combination statutes feature both the benefits and drawbacks of their constituent parts.¹¹⁸ The Interstate Stalking Act includes a specific intent and a reasonable victim standard;¹¹⁹ yet, the usefulness of the Act is limited by the weakness of its specific intent element.¹²⁰ According to the National Center for Victims of Crime, the Act's requirement that the harasser intend to place the victim in reasonable fear of death or serious bodily harm presents a significant evidentiary burden to the government and has led to few federal prosecutions to date.¹²¹

The Appendix to this Note documents current state and federal statutes that could apply to cyberharassment and their constituent elements.¹²² Statutes that include requirements of specific intent and objective reasonableness standards from the victim's perspective are the most common, whereas laws incorporating subjective "reasonable victim" or objective "reasonable harasser" requirements are less so.¹²³ Nevertheless, these statutory schemes, even working in combination, may be inadequate to address the few remedies available to the cyberharassment victim as compared to the instantaneous contact, constant access, anonymity, and other advantages available to cyberharassers.¹²⁴

credible threat with the intent to place that person in reasonable fear for his or her safety . . . is guilty of the crime of stalking."); MO. REV. STAT. § 565.225 (1999 & Supp. 2010) (defining a "credible threat" as a "threat communicated with the intent to cause the person who is the target of the threat to reasonably fear for his or her safety").

¹¹⁸ See *Violence Against Women Act of 1999, Stalking Prevention and Victim Protection Act of 1999: Hearing on H.R. 1248 and H.R. 1869 Before the Subcomm. on Crime of the H. Comm. on the Judiciary*, 106th Cong. 228 (1999) [hereinafter *Hearing on Violence Against Women Act and Stalking Prevention and Victim Protection Act*] (statement by David Beatty, Director of Public Policy for the National Center for Victims of Crime).

¹¹⁹ *Id.* Section 2261(A) reads in applicable part:

Whoever . . .

(2) with the intent—

(A) to kill, injure, harass, or place user surveillance with intent to kill, injure, harass, or intimidate, or cause substantial emotional distress to a person . . . or;

(B) to place a person . . . in reasonable fear of the death of, of serious bodily injury to—

(i) that person;

(ii) a member of the immediate family . . . or;

(iii) a spouse or intimate partner of that person

Id.

¹²⁰ See *Hearing on Violence Against Women Act and Stalking Prevention and Victim Protection Act*, *supra* note 118, at 228.

¹²¹ *Id.*

¹²² See *infra* Appendix.

¹²³ See *infra* Appendix.

¹²⁴ See *1999 Report on Cyberstalking*, *supra* note 23.

Therefore, a different statutory strategy is needed in order to effectively curtail cyberharassment while respecting each party's lawful rights.¹²⁵ Some state and foreign stalking and harassment statutes already incorporate another legal mechanism that could be effective in this regard: burden-shifting devices.¹²⁶

III. AN ALTERNATIVE STRATEGY: STATUTORY BURDEN-SHIFTING DEVICES

In light of the limitations of existing statutory schemes, allocating evidentiary burdens differently between the parties through burden-shifting devices, such as affirmative defenses and nonmandatory presumptions, could be an effective means of reconciling the heavy evidentiary burden placed upon government prosecutors and victims, the free speech rights of online speakers, and the uniquely anonymous and dangerous nature of cyberharassment.¹²⁷ In Part III.A, this Note examines the procedural aspects of affirmative defenses and presumptions in criminal law and their relevant constitutional analyses.¹²⁸ Part III.B then discusses the practical and policy implications of nonmandatory burden-shifting devices, and advocates for the use of such devices in cyberharassment statutes.¹²⁹ Finally, Part III.C surveys existing state and foreign statutes that feature burden-shifting elements, and identifies statutory models that states should emulate when drafting these statutes in order to withstand First and Fourteenth Amendment challenges.¹³⁰

¹²⁵ See *Hearing on Violence Against Women Act and Stalking Prevention and Victim Protection Act*, *supra* note 118, at 228; Lamplugh & Infield, *supra* note 77, at 865; Radosevich, *supra* note 33, at 1384–85; Merschman, *supra* note 13, at 269.

¹²⁶ See KAN. STAT. ANN. § 21-3438 (2007 & Supp. 2009); MICH. COMP. LAWS ANN. §§ 750.411h, .411i (West 2004); MONT. CODE ANN. §§ 45-8-213, 45-5-220 (2009); N.H. REV. STAT. ANN. § 633:3-a (2007); OKLA. STAT. tit. 21 § 1173 (2002); TENN. CODE ANN. § 39-17-315 (2010); VT. STAT. ANN. tit. 13, § 1027 (2009); WASH. REV. CODE ANN. § 9A.46.110 (West 2009); Protection from Harassment Act, 1997, 25 & 26 Eliz. 2, c. 40 (Eng.).

¹²⁷ See *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 341–42, 357 (1995); Miller et al., *supra* note 52, at 82; Wolak et al., *supra* note 28, at S52.

¹²⁸ See *infra* notes 131–164 and accompanying text.

¹²⁹ See *infra* notes 165–221 and accompanying text.

¹³⁰ See *infra* notes 222–257 and accompanying text.

A. *Procedural Aspects of Burden-Shifting Devices and Propriety
Under the Constitution*

Burden-shifting devices are a common feature of civil and criminal law that reallocate the burden of production,¹³¹ the burden of persuasion,¹³² or both¹³³ from the prosecution to the accused with regard to an element of the offense or to mitigate liability.¹³⁴ Burden shifting is typically embodied in two types of procedural devices: affirmative defenses and presumptions.¹³⁵

Affirmative defenses place the evidentiary burden on the accused to come forward with exculpatory facts to limit or negate his or her criminal liability, even if the prosecution has successfully demonstrated the elements of the offense.¹³⁶ These defenses, which are included in many modern criminal statutes, can shift the burden of production, the burden of persuasion, or both to the accused.¹³⁷ Although some academics debate whether affirmative defenses are consistent with the criminal standard of proof—guilt beyond a reasonable doubt—these devices have not been subjected to significant criticism on constitutional grounds.¹³⁸

¹³¹ Leslie J. Harris, *Constitutional Limits on Criminal Presumptions as an Expression of Changing Concepts of Fundamental Fairness*, 77 J. CRIM. L. & CRIMINOLOGY 308, 308, 310 (1986). The party bearing the burden of production has the obligation of raising an issue and presenting sufficient evidence to get to the jury. *Id.* If the party cannot meet its burden of production, the judge will resolve the issue against that party via directed verdict. *Id.*

¹³² *Id.* The party bearing the burden of persuasion, typically the government in a criminal proceeding, has the responsibility of convincing the factfinder of the truthfulness of that party's assertions. *Id.* Whether a party has satisfied its burden of persuasion is determined after the factfinder considers all available evidence against the proper standard of proof; if the factfinder remains uncertain, the issue is resolved against that party. John Calvin Jeffries, Jr. & Paul B. Stephan III, *Defenses, Presumptions, and Burden of Proof in Criminal Law*, 88 YALE L.J. 1325, 1329 n.8 (1979). Devices that assign the burden of persuasion are sometimes called "assumptions." See Harold A. Ashford & D. Michael Risinger, *Presumptions, Assumptions, and Due Process in Criminal Cases*, 79 YALE L.J. 165, 173 (1969).

¹³³ See Ashford & Risinger, *supra* note 132, at 173. The term "burden of proof" is often used imprecisely and may refer to either or both the burdens of production and persuasion. *Id.* For the purposes of this Note, "burden of proof" generally refers to both burdens, and the individual burdens are specifically identified.

¹³⁴ Harris, *supra* note 131, at 314.

¹³⁵ See Jeffries & Stephan, *supra* note 132, at 1327.

¹³⁶ See *id.*

¹³⁷ See *id.* at 1329–30.

¹³⁸ See *id.* at 1335, 1336; Peter D. Bewley, Note, *The Unconstitutionality of Statutory Criminal Presumptions*, 22 STAN. L. REV. 341, 343 n.21 (1970) ("The import of the language appears to be that a procedure shifting to the defendant the burden of proof on an element of the crime would be unconstitutional, while one putting the burden of proof of an affirmative defense on him is not.").

Presumptions allow one fact to be inferred by evidence of another and are also widely used as burden-shifting devices.¹³⁹ They are particularly prevalent in statutes targeting the possession of weapons, alcohol, narcotics, or other areas of heightened public and legislative concern.¹⁴⁰ Although the terminology used to differentiate between types of presumptions varies, the U.S. Supreme Court officially recognized two categories of presumptions in its 1979 decision in *County Court v. Allen*: mandatory presumptions and nonmandatory presumptions.¹⁴¹ Mandatory presumptions, also called “true” or “conclusive” presumptions, require the factfinder to draw an inference from available evidence unless the defendant can rebut it.¹⁴² Nonmandatory presumptions, also called “permissive presumptions” or “permissive inferences,” allow the factfinder to infer one fact from proof of another, but the presumption is not compulsory.¹⁴³ Presumptions are also classified according to whether they shift the burden of production or the burden of persuasion.¹⁴⁴

Unlike affirmative defenses, presumptions have been attacked on constitutional grounds since the nineteenth century and the Supreme Court has in fact deemed certain kinds of presumptions as unconstitutional *per se*.¹⁴⁵ In 1975, the Court held in *Mullaney v. Wilbur* that pre-

¹³⁹ See BLACK'S LAW DICTIONARY 1304 (9th ed. 2009) (defining “presumption” as “[a] legal inference or assumption that a fact exists, based on the known or proven existence of some other fact or group of facts”); Jeffries & Stephan, *supra* note 132, at 1327. Although prevalent in statutory law, the very nature of presumptions is contested; they have been characterized as rules of law, procedure, evidence, or a combination of all three. See Julian P. Alexander, *Presumptions: Their Use and Abuse*, 17 Miss. L.J. 1, 3 n.6 (1945).

¹⁴⁰ See Allen Fuller & Robert Urich, *An Analysis of the Constitutionality of Statutory Presumptions That Lessen the Burden of the Prosecution*, 25 U. MIAMI L. REV. 420, 420 (1971); Jeffries & Stephan, *supra* note 132, at 1326, 1335; see, e.g., Turner v. United States, 396 U.S. 398, 400 (1970) (heroin); Leary v. United States, 395 U.S. 6, 9 (1969) (marijuana); United States v. Gainey, 380 U.S. 63, 64 (1965) (alcohol); United States v. Romano, 382 U.S. 136, 137 (1965) (alcohol); Tot v. United States, 319 U.S. 463, 464 (1943) (firearms).

¹⁴¹ See 442 U.S. 140, 157 (1979) (dividing presumptions and inferences into two categories: permissive and mandatory).

¹⁴² See Alexander, *supra* note 139, at 4–5; Jeffries & Stephan, *supra* note 132, at 1335. Some legal scholars distinguish “conclusive” presumptions from mandatory presumptions, defining the former as foreclosing any further argument once certain facts are shown. See Neil S. Hecht & William M. Pinzler, *Rebutting Presumptions: Order out of Chaos*, 58 B.U. L. REV. 527, 529 (1978); Bewley, *supra* note 138, at 342.

¹⁴³ See Harris, *supra* note 131, at 310; Jeffries & Stephan, *supra* note 132, at 1335–36; Bewley, *supra* note 138, at 343. This classification of presumptions is complicated further by the practice of some courts to construe presumptions with mandatory language as if the presumption were not required. See Jeffries & Stephan, *supra* note 132, at 1335–36.

¹⁴⁴ See Bewley, *supra* note 138, at 343.

¹⁴⁵ See *Mullaney v. Wilbur*, 421 U.S. 684, 703–04 (1975) (finding unconstitutional a rebuttable presumption that shifted the burden of persuasion to the defendant, on the

sumptions that transfer the burden of persuasion to the defendant violate the Due Process Clause of the Fourteenth Amendment.¹⁴⁶ The Court has also criticized mandatory presumptions, in dicta, as violative of the defendant's right to have a trial jury consider all elements of an offense, on the grounds that mandatory presumptions compel (rather than permit) the factfinder to draw inferences from proven evidence.¹⁴⁷

In the aftermath of *Mullaney*, only rebuttable, nonmandatory presumptions that affect the burden of production are permissible in criminal law.¹⁴⁸ Consequently, only this category of presumption has further utility for cyberharassment statutes.¹⁴⁹ Rebuttable, nonmandatory presumptions allow the prosecution to introduce prima facie evidence that switches the burden of production to the defendant to produce sufficient evidence to invalidate the presumption.¹⁵⁰ If the presumption is successfully rebutted, the burden of production shifts back to the prosecution to fully prove the fact at issue.¹⁵¹ If the defendant cannot over-

grounds that due process requires the prosecution to prove the elements of the crime beyond a reasonable doubt); Harris, *supra* note 131, at 308.

¹⁴⁶ See 421 U.S. at 703.

¹⁴⁷ See, e.g., *Sandstrom v. Montana*, 442 U.S. 510, 521–23 (1979) (quoting *United States v. U.S. Gypsum Co.*, 438 U.S. 442, 446 (1978)) (“[A] conclusive presumption in this case would . . . ‘invade [the] factfinding function’ which in a criminal case the law assigns solely to the jury.”); *U.S. Gypsum Co.*, 438 U.S. at 446 (ruling that a conclusive presumption in a criminal antitrust action was impermissible because “ultimately the decision on the issue of intent must be left to the trier of fact alone”); *Morisette v. United States*, 342 U.S. 246, 275 (1952) (“A conclusive presumption which testimony could not overthrow would effectively eliminate intent as an ingredient of the offense.”).

Under these analyses, a presumption that if A and B are proved, then C is also proved, violates due process because the jury is not given the choice of whether to infer C. See *Ashford & Risinger*, *supra* note 132, at 175. This reasoning remains unchanged even if the defendant is given the opportunity to rebut the mandatory presumption because if the defendant fails to invalidate the presumption, the disputed fact is nevertheless resolved automatically against him or her. See *id.* This results in the equivalent of a directed verdict against the accused, which is impermissible in criminal law. See *Bewley*, *supra* note 138, at 343.

Additionally, presumptions that operate in an unreasonable or capricious manner or circumvent substantive constitutional rights violate due process requirements under the Fifth and Fourteenth Amendments. See *Bailey v. Alabama*, 219 U.S. 219, 239 (1911) (“The power to create presumptions is not a means of escape from constitutional restrictions.”); *Mobile, Jackson & Kansas City R.R. Co. v. Turnipseed*, 219 U.S. 35, 43 (1910) (“[T]he inference of one fact from proof of another shall not be so unreasonable as to be a purely arbitrary mandate.”).

¹⁴⁸ See *Mullaney*, 421 U.S. at 703–04; Hecht & Pinzler, *supra* note 142, at 529; *Bewley*, *supra* note 138, at 343.

¹⁴⁹ See *Mullaney*, 421 U.S. at 703–04; Hecht & Pinzler, *supra* note 142, at 529; *Bewley*, *supra* note 138, at 343.

¹⁵⁰ See *Ashford & Risinger*, *supra* note 132, at 174.

¹⁵¹ See *id.*

come the presumption, the factfinder is given the option to infer the existence of the presumed fact from the facts already proven.¹⁵² Critically, however, even presumptions that survive the *Mullaney* standard must also satisfy two additional constitutional tests to comply with due process: (1) the rational connection test, as first introduced by the Supreme Court in the 1910 case of *Mobile, Jackson & Kansas City Railroad Co. v. Turnipseed*, and (2) the comparative convenience test, as articulated by the Court in the 1934 case of *Morrison v. California*.¹⁵³

The rational connection test is considered the dominant analysis for determining the constitutionality of nonmandatory presumptions.¹⁵⁴ When first formulating the test in *Turnipseed*, the Supreme Court held that a legislative presumption does not violate due process or equal protection requirements so long as there is some rational connection between the fact proved and the fact presumed.¹⁵⁵ Additionally, the party against whom the presumption operates must not be precluded from presenting his or her own evidence for the purpose of rebuttal.¹⁵⁶ The rational connection test was subsequently refined in the Supreme Court's 1969 decision in *Leary v. United States*, where the Court determined that a presumption satisfies the rational connection test if "it can at least be said with substantial assurance that the presumed fact is more likely than not to flow from the proved fact on which it is made to depend."¹⁵⁷

¹⁵² See *id.*

¹⁵³ See *Morrison v. California*, 291 U.S. 82, 88–91 (1934); *Turnipseed*, 219 U.S. at 43. The U.S. Supreme Court also proposed a third due process test for presumptions in its 1928 decision *Ferry v. Ramsey*, termed "the greater includes the lesser" rule. See 277 U.S. 88, 94 (1928). The reasoning behind this rule is as follows: if the legislature could constitutionally punish a crime featuring elements A and B, a statute that permits element C to be presumed from elements A and B is also constitutional because this presumption provides the defendant with an opportunity to escape conviction even if A and B are proven. See *id.*; Ashford & Risinger, *supra* note 132, at 177. This is because the permissible inference of element C can be rebutted. See Ashford & Risinger, *supra* note 132, at 177. In comparison to the rational connection and comparative convenience tests, however, commentators consider the "greater includes the lesser" theory defunct because the Supreme Court declined to apply the rule in the 1965 decision *United States v. Romano*, instead employing the rational connection test. See 382 U.S. at 144; Ashford & Risinger, *supra* note 132, at 178.

¹⁵⁴ See Ashford & Risinger, *supra* note 132, at 166.

¹⁵⁵ 219 U.S. at 43.

¹⁵⁶ *Id.*

¹⁵⁷ 395 U.S. at 36 (ruling unconstitutional, under the rational connection test, a criminal statutory presumption that authorized the jury to infer from a defendant's possession of marijuana that the marijuana had been imported into the United States illegally and that the defendant knew of the unlawful importation). Some commentators disapprove of the rational connection test, alleging that it disregards substantive issues in favor of a formalistic, empirical search for a logical connection between proven and presumed facts. See

The second constitutional test for presumptions, the comparative convenience test, acts as a corollary or threshold analysis for the rational connection test.¹⁵⁸ Justice Cardozo first introduced the comparative convenience analysis in *Morrison*, which allowed the burden of proof to be transferred to the defendant if the inconvenience to the defendant is less than the benefit to the prosecution.¹⁵⁹ In *Morrison*, Justice Cardozo reasoned:

The decisions are manifold that within limits of reason and fairness the burden of proof may be lifted from the state in criminal prosecutions and cast on a defendant. The limits are in substance these, that the state shall have proved enough to make it just for the defendant to be required to repel what has been proved with excuse or explanation, or at least that upon a *balancing of convenience* or of the opportunities for knowledge the shifting of the burden will be found to be an aid to the accuser without subjecting the accused to hardship or oppression.¹⁶⁰

The *Morrison* Court may have been influenced by the views of evidence scholar John Henry Wigmore, who envisioned presumptions as devices for distributing, instead of satisfying, burdens of proof.¹⁶¹ Pursuant to this test, burden shifting is permissible and even proper where there are significant disparities in convenience of proof and opportunities for knowledge between the parties.¹⁶² The combination of the comparative convenience and rational connection tests implies that a court will be less critical of the connection between the state's evidence and the presumed fact if the circumstances are such that the prosecution would be seriously disadvantaged by an obligation to affirmatively support the presumption.¹⁶³ Although a corollary test, the comparative convenience rule remains relevant in the constitutional analysis of presumptions and, as discussed in Part III.B, parallels issues inherent in cyberharassment

Ashford & Risinger, *supra* note 132, at 166–67; Harris, *supra* note 131, at 328–29; 333–34; Jeffries & Stephan, *supra* note 132, at 1396.

¹⁵⁸ See *Tol*, 319 U.S. at 467; Ashford & Risinger, *supra* note 132, at 180.

¹⁵⁹ See 291 U.S. at 88; Ashford & Risinger, *supra* note 132, at 168.

¹⁶⁰ 291 U.S. at 88–89 (emphasis added).

¹⁶¹ Harris, *supra* note 131, at 320–21; see *Morrison*, 291 U.S. at 88–89 (citing 5 JOHN WIGMORE, EVIDENCE 2486, 2512 (2d ed. 1923)).

¹⁶² See *Morrison*, 291 U.S. at 90–91.

¹⁶³ Ashford & Risinger, *supra* note 132, at 168.

cases; namely, the inequality of information and “opportunities for knowledge” between cyberharassers and their victims.¹⁶⁴

B. *Comparative Convenience and Fundamental Fairness: Burden-Shifting Devices as Balancing Mechanisms*

Notwithstanding the constitutional scrutiny imposed under *Mullaney* and the rational connection and comparative convenience tests, statutory burden-shifting devices have the greatest utility for offenses where the legislature believes that it is practical, convenient, and fair to lessen the initial burden of proof required from the state.¹⁶⁵ This burden is then transferred to the accused to present evidence in order to rationalize his or her actions.¹⁶⁶

Affirmative defenses and nonmandatory presumptions are well suited for ameliorating the evidentiary difficulties that make cyberharassment cases so arduous for victims and government prosecutors, consistent with their use as vehicles for increased fairness and efficiency in other areas of the criminal law.¹⁶⁷ State and federal legislatures should increase the efficacy of their cyberharassment laws by supplementing typical statutory elements, such as standards of reasonableness and specific intent, with nonmandatory burden-shifting devices that reallocate part of the burden of proof to the defendant.¹⁶⁸ Such devices would better account for the realistic difficulties of obtaining proof of anonymous or pseudonymous harassment and balance the interests of both parties by providing justice for victims without compromising the free speech or due process rights of the accused.¹⁶⁹ In order to weigh the merits of this theory, a more detailed review of the practical advantages and disadvantages of burden shifting is necessary.¹⁷⁰

¹⁶⁴ See *Morrison*, 291 U.S. at 88–91; *infra* notes 195–202 and accompanying text.

¹⁶⁵ See *Leary*, 395 U.S. at 36; *Morrison*, 291 U.S. at 88.

¹⁶⁶ See Ashford & Risinger, *supra* note 132, at 174; Jeffries & Stephan, *supra* note 132, at 1327.

¹⁶⁷ See Alexander, *supra* note 139, at 2; Joseph P. Chamberlain, *Presumptions as First Aid to the District Attorney*, 14 A.B.A. J. 287, 287, 288 (1928); Jeffries & Stephan, *supra* note 132, at 1334, 1354; Barbara D. Underwood, *The Thumb on the Scales of Justice: Burdens of Persuasion in Criminal Cases*, 86 YALE L.J. 1299, 1321, 1335–36 (1977).

¹⁶⁸ See Alexander, *supra* note 139, at 2; Chamberlain, *supra* note 167, at 287, 288; Jeffries & Stephan, *supra* note 132, at 1334, 1354; Underwood, *supra* note 167, at 1321, 1335–36.

¹⁶⁹ See *Morrison*, 291 U.S. at 88–91; Jeffries & Stephan, *supra* note 132, at 1355; Miller et al., *supra* note 52, at 82.

¹⁷⁰ See Alexander, *supra* note 139, at 2; Fuller & Urich, *supra* note 140, at 421–24; Underwood, *supra* note 167, at 1321, 1323–35.

1. Advantages of Burden-Shifting Devices in Cyberharassment Law

Burden-shifting mechanisms are useful for facilitating efficient litigation in areas of the criminal law where the prosecution is placed at a substantial procedural disadvantage, and have long been used in such a way.¹⁷¹ Presumptions and inferences reduce judicial costs by formalizing recognized patterns of circumstantial evidence, based on observation and experience, in order to establish one related fact from proof of another.¹⁷² Burden shifting is commonly employed as an aid for prosecutors where the government must prove criminal elements related to state of mind or intent, and such facts lie peculiarly within the knowledge of the accused.¹⁷³ A state's inclusion of burden-shifting devices within criminal statutes indicates a legislative choice to facilitate convictions by easing the prosecution's burden of proof—the trier of fact is permitted to draw certain inferences from a lesser quantum of evidence that would not normally meet the standard of proof of beyond a reasonable doubt.¹⁷⁴ Notwithstanding additional due process considerations for presumptions, affirmative defenses and presumptions that shift the burden of production to the defendant are generally considered acceptable housekeeping mechanisms for screening out extraneous issues and eliciting evidence to which the defendant has special access, without substantially increasing the risk of false convictions.¹⁷⁵

Burden-shifting devices are also justified for reasons of public policy.¹⁷⁶ Such devices encourage reform of penal law and grant legislatures greater leeway in the statutory definition of crimes, allowing them to draft the offense in expansive language in order to sweep in the

¹⁷¹ See Alexander, *supra* note 139, at 2.

¹⁷² See *id.*

¹⁷³ See *id.*; Chamberlain, *supra* note 167, at 288.

¹⁷⁴ See Harris, *supra* note 131, at 325; Note, *Statutory Criminal Presumptions: Judicial Sleight of Hand*, 53 VA. L. REV. 702, 702–04 (1967) [hereinafter *Judicial Sleight of Hand*]. Presumptions have been characterized as “an instinctive response to counterbalance the expanding constitutional protections afforded criminal defendants by the courts” and assist prosecutors in two ways by: (1) allowing prosecutors to avoid demonstrating criminal elements that are inherently difficult to establish and in practice, almost impossible to prove; and (2) allowing prosecutors to avoid producing evidence that is easily accessible to the defendant but extremely inconvenient for the state to obtain. *Judicial Sleight of Hand*, *supra*, at 702–04.

¹⁷⁵ See Jeffries & Stephan, *supra* note 132, at 1334; Underwood, *supra* note 167, at 1335–36; *Judicial Sleight of Hand*, *supra* note 174, at 705. Burden shifting devices that reallocate the burden of production have been employed successfully for defenses such as insanity, duress, entrapment, abandonment, and choice of evils. Underwood, *supra* note 167, at 1335–36.

¹⁷⁶ See Alexander, *supra* note 139, at 2; see Fuller & Urich, *supra* note 140, at 429; Jeffries & Stephan, *supra* note 132, at 1354; Underwood, *supra* note 167, at 1321.

maximum number of offenders.¹⁷⁷ Burden-shifting mechanisms then ameliorate broad legislative drafting by providing an escape hatch, or substantive compromise, for less culpable individuals who acted from legitimate motives, without fault, or are otherwise unsuitable for criminal sanctions.¹⁷⁸ Consequently, one of the primary benefits of affirmative defenses is their amelioration of the harshness of criminal law and their prevention of injustice.¹⁷⁹

Legal mechanisms that reallocate the burden of proof are of greatest use for offenses where the prosecution lacks access to evidence involving the defendant's intent or other facts peculiarly within the defendant's knowledge.¹⁸⁰ It follows that burden-shifting devices could effectively be applied to the area of cyberharassment, in which initial evidentiary burdens, particularly with regard to the alleged harasser's mental state, can be almost insurmountable for the state, leaving victims with no legal recourse.¹⁸¹

Part of the difficulty of prosecuting technology-savvy harassers is the ease with which defendants can harm the victim.¹⁸² Cyberharassers have the capability to invade the victim's privacy, destroy his or her reputation, and inflict financial, psychological or even physical harm from great distances.¹⁸³ Additionally, because of statutory disincentives for ISP disclosure of IP addresses and harassers' propensity to supply false identification information, anonymous or pseudonymous harassers can evade law enforcement with minimal effort.¹⁸⁴

Victims' burdens are further compounded if applicable statutes employ reasonableness or intent requirements that are extremely protective of the electronic marketplace of ideas and the defendant's speech and due process rights.¹⁸⁵ Courts' reluctance to exclude offen-

¹⁷⁷ See Fuller & Ulrich, *supra* note 140, at 429; Underwood, *supra* note 167, at 1321. *But see* Ashford & Risinger, *supra* note 132, at 191 (arguing that the definition of a crime should not be so broad that large numbers of individuals fall into the exceptions to liability generated by affirmative defenses, as the criminal law should discourage not only unlawful conviction, but also the erroneous arrest and trial of innocent persons).

¹⁷⁸ See Fuller & Ulrich, *supra* note 140, at 429; Underwood, *supra* note 167, at 1321.

¹⁷⁹ See Jeffries & Stephan, *supra* note 132, at 1354.

¹⁸⁰ See Harris, *supra* note 131, at 325; Jeffries & Stephan, *supra* note 132, at 1334; Underwood, *supra* note 167, at 1335; *Judicial Sleight of Hand*, *supra* note 174, at 703–04.

¹⁸¹ See Harris, *supra* note 131, at 325; Jeffries & Stephan, *supra* note 132, at 1334; Underwood, *supra* note 167, at 1335; *Judicial Sleight of Hand*, *supra* note 174, at 703–04.

¹⁸² See *1999 Report on Cyberstalking*, *supra* note 23.

¹⁸³ See *id.*

¹⁸⁴ See 47 U.S.C. § 230(c) (2006); *1999 Report on Cyberstalking*, *supra* note 23; Miller et al., *supra* note 52, at 82.

¹⁸⁵ See Lamplugh & Infield, *supra* note 77, at 865.

sive communications, group defamation, and hate speech from First Amendment protection to preserve the autonomy of even unpopular speakers indicates the extent of judicial abhorrence to nearly all forms of censorship, regardless of whether the regulated speech is low in social value.¹⁸⁶ Consequently, the constitutional analysis in cyberharassment cases is inherently protective of the harasser.¹⁸⁷ Only where speech escalates to the level of intimidation or threats that places the victim in genuine fear of bodily harm do the safety interests of the victim override the speaker's right to free expression.¹⁸⁸

Many state and federal legislatures have encountered difficulty in drafting criminal cyberharassment statutes precisely because the scope of possible conduct is so broad and may include constitutionally protected speech.¹⁸⁹ Expansive statutes that sweep in antisocial but expressive conduct, such as online taunting between classmates, will likely be invalidated for overbreadth or vagueness.¹⁹⁰ Such actions are legally permissible and at worst, better addressed by guardians, schools, and even civil courts rather than the criminal justice system.¹⁹¹ Statutes that are worded too narrowly, however, will not be effective against nontraditional but

¹⁸⁶ See, e.g., *NAACP v. Claiborne Hardware Co.*, 458 U.S. 886, 910 (1982) (“Speech does not lose its protected character . . . simply because it may embarrass others or coerce them into action.”); *Cohen v. California*, 403 U.S. 15, 21 (1971); *Feiner v. New York*, 340 U.S. 315, 331 (1951) (Douglas, J., dissenting) (“[S]peakers need police protection. If they do not receive it . . . the police become the new censors of speech. Police censorship has all the vices of the censorship from city halls which we have repeatedly struck down.”); *Cantwell v. Connecticut*, 310 U.S. 296, 310 (1940) (“To persuade others to his own point of view, the pleader . . . resorts to exaggeration, to vilification . . . and even to false statement. But . . . these liberties are . . . essential to enlightened opinion and right conduct on the part of the citizens of a democracy.”).

¹⁸⁷ See, e.g., *Claiborne Hardware Co.*, 458 U.S. at 910; *Cohen*, 403 U.S. at 21; *Cantwell*, 310 U.S. at 310.

¹⁸⁸ See *Virginia v. Black*, 538 U.S. 343, 344 (2003) (“Intimidation . . . is a type of true threat, where a speaker directs a threat to a person or group of persons with the intent of placing the victim in fear of bodily harm or death.”); *Watts v. United States*, 394 U.S. 705, 707–08 (1969) (per curiam) (“What is a threat must be distinguished from what is constitutionally protected speech.”); *Thorne v. Bailey*, 846 F.2d 241, 243 (4th Cir. 1988) (quoting *State v. Thorne*, 333 S.E.2d 817, 819 (W. Va. 1985)) (“Prohibiting harassment is not prohibiting speech, because harassment is not a [*sic*] protected speech. Harassment is not communication, although it may take the form of speech.”).

¹⁸⁹ See *Hearing on Megan Meier Cyberbullying Prevention Act and AWARE Act*, *supra* note 93, at 23 (statement of Hon. Linda T. Sánchez) (“I want the [Megan Meier Cyberbullying Prevention Act] to be able to distinguish between an annoying chain email, a righteous angry political blog post, or a miffed text to an ex-boyfriend—all of which should remain legal; and serious, repeated, and hostile communications made with the intent to harm.”).

¹⁹⁰ See *State v. Johnson*, 191 P.3d 665, 668 (Or. 2008).

¹⁹¹ See *Dickerson*, *supra* note 22, at 70–74; *Lamplugh & Infield*, *supra* note 77, at 866.

dangerous means of online harassment, such as stalking by proxy.¹⁹² Burden-shifting mechanisms allow greater leeway in statutory drafting for sui generis offenses like cyberharassment because they expand the reach of the statute to encompass many forms of harassment without increasing the risk of constitutional invalidation or false conviction.¹⁹³ Additionally, presumptions and affirmative defenses can be easily tailored to particular offenses, which makes them well suited to “upgrade criminal procedures” in response to constantly evolving cybercrimes.¹⁹⁴

Incorporation of burden-shifting devices within cyberharassment statutes also makes sense on a policy level.¹⁹⁵ In fact, the practical concerns of cyberharassment cases mirror the issues that gave rise to Justice Cardozo’s comparative convenience test for presumptions in *Morrison*.¹⁹⁶ Where convenience of proof and opportunities for knowledge vary greatly between the prosecution and the defense, the legislature may permissibly transfer a portion of the burden of proof in order to balance the interests of both parties.¹⁹⁷ This process is not for the purpose of obtaining convictions more easily or quickly, but instead to facilitate more efficient prosecution and impose criminal sanctions upon sufficiently culpable parties where the prosecution might otherwise be exceedingly difficult due to lack of available information.¹⁹⁸ This Note does not advocate for a prosecution-oriented approach to cyberharassment.¹⁹⁹ Rather, it recognizes that cyberharassment victims are already at a significant disadvantage when attempting to identify their harass-

¹⁹² See Goodno, *supra* note 1, at 132, 140; Zeller, *supra* note 34.

¹⁹³ See Harris, *supra* note 131, at 325; Jeffries & Stephan, *supra* note 132, at 1334; Underwood, *supra* note 167, at 1335–36; *Judicial Sleight of Hand*, *supra* note 174, at 702–04.

¹⁹⁴ See *Judicial Sleight of Hand*, *supra* note 174, at 702.

¹⁹⁵ See *Morrison*, 291 U.S. at 88–91.

¹⁹⁶ See *id.*

¹⁹⁷ See *id.* at 90–91.

¹⁹⁸ See Ashford & Risinger, *supra* note 132, at 186; Bewley, *supra* note 138, at 354.

¹⁹⁹ Cf. Fuller & Urich, *supra* note 140, at 427; Bewley, *supra* note 138, at 354–55. These commentators view presumptions as an unconstitutional, accusatorial shortcut that gives short shrift to the criminal defendant and due process in favor of easing the burden on prosecutors and the criminal justice system. See Fuller & Urich, *supra* note 140, at 427; Bewley, *supra* note 138, at 354–55. This view has been stated by jurists as well, such as Justice McReynolds in his dissent to the 1928 U.S. Supreme Court decision, *Casey v. United States*:

Once the thumbscrew and the following confession made conviction easy; but that method was crude and, I suppose, now would be declared unlawful upon some ground. Hereafter, presumption is to lighten the burden of the prosecutor. The victim will be spared the trouble of confessing and will go to his cell without mutilation or disquieting outcry.

ers, let alone prove their intent or state of mind beyond a reasonable doubt.²⁰⁰ These elements lie peculiarly within the knowledge of the accused.²⁰¹ Sharing evidentiary burdens between victims and defendants should harmonize the interests of both sides, rather than overwhelmingly favor one side over the other.²⁰²

2. Disadvantages and Constitutional Objections to Burden-Shifting Devices

Burden-shifting devices are certainly not perfect. As discussed in Part III.A, the use of affirmative defenses and particularly presumptions has historically raised issues of constitutionality with regard to due process, the constitutional privilege against self incrimination, and the right to a trial by jury for the defendant.²⁰³ Commentators' principal objection against these devices concerns their reduction of the prosecution's constitutional burden of proving every element of the crime beyond a reasonable doubt.²⁰⁴ Burden-shifting mechanisms permit cer-

²⁰⁰ See *1999 Report on Cyberstalking*, *supra* note 23; Miller et al., *supra* note 52, at 82.

²⁰¹ See Alexander, *supra* note 139, at 2; Chamberlain, *supra* note 167, at 287–88.

²⁰² See Alexander, *supra* note 139, at 2; Chamberlain, *supra* note 167, at 287–88.

²⁰³ See Fuller & Urlich, *supra* note 140, at 421–24. Justice Black enumerated several constitutional arguments against presumptions in his dissent in the U.S. Supreme Court's 1970 opinion in *Turner v. United States*, including: (1) the defendant's right not to be compelled to answer for a capital or otherwise infamous crime unless on a presentment or indictment of a grand jury; (2) the defendant's right to be informed of the nature and cause of the accusation against him or her; (3) the right not to be compelled to be a witness against oneself; (4) the right not to be deprived of life, liberty, or property without due process of law; (5) the defendant's right to be confronted with the witnesses against him or her; (6) the right to compulsory process for obtaining witnesses for one's defense; (7) the right to counsel; and (8) the right to trial by an impartial jury. 396 U.S. at 425 (Black, J., dissenting). Several of these arguments have since been rejected. See Fuller & Urlich, *supra* note 140, at 424.

Another noteworthy argument against presumptions involves their effect on the decisionmaking roles of the judge and jury and the description of permissible inferences in jury instructions, even if the presumption itself satisfies the rational connection test. See Harris, *supra* note 131, at 311. This issue culminated in 1979 in *Sandstrom v. Montana*, in which the U.S. Supreme Court, after discussing *Morissette* and *U.S. Gypsum Co.*, held that whether a presumption is unconstitutional as a mandatory or "conclusive" presumption, or a presumption that impermissibly shifts the burden of persuasion to the defendant, depends upon a reasonable jury's interpretation of the jury instructions. *Sandstrom*, 442 U.S. at 524. If the instructions have a conclusive or persuasion-shifting effect, then the presumption is unconstitutional. *Id.* at 523–24.

²⁰⁴ See *In re Winship*, 397 U.S. 358, 364 (1970) (holding that the Due Process Clause requires the prosecution to present proof beyond a reasonable doubt of "every fact necessary to constitute the crime with which [the accused] is charged"). When the Supreme Court decided *In re Winship* in 1970, commentators did not consider the decision particularly innovative, as all American courts already employed the criminal standard of proof

tain facts to be inferred by the factfinder rather than affirmatively proven by the government.²⁰⁵ These devices, commentators argue, create an insufficient factual basis for punishment and increase the risk of erroneous conviction, which the demanding reasonable doubt standard was intended to safeguard against.²⁰⁶

Jurists and commentators have also criticized the practical benefits of presumptions, arguing that judicial efficiency or any evidentiary hardship imposed upon the state do not justify shifting the burden of proof away from the prosecution.²⁰⁷ Commentators contend that reassigning evidentiary burdens may result in a slippery slope: the state could theoretically define a crime in extremely general terms and then require the defendant to show that he acted without a culpable mental state, completely freeing the prosecution from proving *mens rea*.²⁰⁸ Shifting the burden to the defendant to justify or excuse his conduct could result in disproportionately harsh penalties and substantial injustice.²⁰⁹ Furthermore, the existence of “unusual rules of proof” that real-

beyond a reasonable doubt. See Jeffries & Stephan, *supra* note 132, at 1328 (“As a general rule of criminal procedure . . . *Winship* merely confirmed the status quo.”). Nonetheless, *Winship*’s mandate that the reasonable doubt standard be applied to “every fact necessary to constitute the crime . . . charged” has significant implications for burden shifting devices, which transfer the burden of proof for certain facts onto the accused. See *Winship*, 397 U.S. at 364 (emphasis added); Jeffries & Stephan, *supra* note 132, at 1333. Theoretically, if *Winship* were applied to every fact pertaining to a crime, not just its official elements, such a purely procedural approach would invalidate all presumptions and affirmative defenses in criminal law. See Jeffries & Stephan, *supra* note 132, at 1333, 1344. This interpretation was explicitly rejected by the Supreme Court in 1977 in *Patterson v. New York*, where the Court limited the application of *Winship* and *Mullaney* to only those facts identified as formal elements of a crime, rather than all facts affecting “the degree of criminal culpability.” See *Patterson v. New York*, 432 U.S. 197, 215 & n.15 (1977).

²⁰⁵ See Alexander, *supra* note 139, at 1–2 (“[I]t is logical to consider all presumptions as inferences of fact.”); Harris, *supra* note 131, at 310, 336 (“A presumption is a rule of law requiring that once some fact (a ‘basic’ or ‘proven’ fact) is established, some other fact at issue (the ‘presumed’ fact) must be deemed true, at least provisionally.”).

²⁰⁶ See *Winship*, 397 U.S. at 372 (Harlan, J., concurring) (“I view the requirement of proof beyond a reasonable doubt in a criminal case as bottomed on a fundamental value determination of our society that it is far worse to convict an innocent man than to let a guilty man go free.”); Fuller & Urich, *supra* note 140, at 422, 427; Jeffries & Stephan, *supra* note 132, at 1346; Bewley, *supra* note 138, at 349.

²⁰⁷ See *Mullaney*, 421 U.S. at 702 (“[A]lthough intent is typically considered a fact peculiarly within the knowledge of the defendant, this does not, as the Court has long recognized, justify shifting the burden to him.”); *Tol*, 319 U.S. at 469 (“Nor can the fact that the defendant has the better means of information, standing alone, justify the creation of such a presumption.”); Bewley, *supra* note 138, at 355 (“The argument from convenience is, in any event, not persuasive since it has never been agreed that an unconstitutional act should be permitted because it is more economical.”).

²⁰⁸ See *Patterson*, 432 U.S. at 224 n.8 (Powell, J., dissenting).

²⁰⁹ See Jeffries & Stephan, *supra* note 132, at 1357.

locate the burden of proof away from the government may mislead potential offenders as to procedural and substantive aspects of the law, raises issues of fair notice, and frustrates the purpose of the criminal law as a guide to public conduct.²¹⁰

As with all statutory mechanisms, burden-shifting devices are imperfect, but this is insufficient grounds for disregarding them as useful tools in cyberharassment litigation.²¹¹ Statutory presumptions and inferences are criticized for their conflict with the presumption of innocence and other privileges granted by the Fifth and Fourteenth Amendments.²¹² This criticism, however, operates primarily on a doctrinal level with the recognition that affirmative defenses and presumptions, in spite of academic misgivings, have long been utilized in penal law and are unlikely to be discontinued.²¹³ Objections to burden-shifting devices as violations of other constitutional rights beyond due process, such as the privilege against self-incrimination, have largely been rejected by courts.²¹⁴ Similarly, contentions that presumptions and defenses lead to injustice are subject to equally persuasive counterarguments that pro-

²¹⁰ Underwood, *supra* note 167, at 1323–25. *But see* Jeffries & Stephan, *supra* note 132, at 1351, 1390–91 (arguing that affirmative defenses have no deceptive effect and that presumptions are only confusing to the extent that they qualify language elsewhere in the statute).

²¹¹ *See* Turner, 396 U.S. at 425 (Black, J., dissenting); Fuller & Urich, *supra* note 140, at 421–25; Bewley, *supra* note 138, at 355.

²¹² *See* Turner, 396 U.S. at 425 (Black, J., dissenting); Fuller & Urich, *supra* note 140, at 421–25; Bewley, *supra* note 138, at 355.

²¹³ *See, e.g.,* Yee Hem v. United States, 268 U.S. 178, 185 (1925) (“Every accused person, of course, enters upon his trial clothed with the presumption of innocence. But that presumption may be overcome, not only by direct proof . . . [but also] by the additional weight of a countervailing legislative presumption.”); Harris, *supra* note 131, at 340 n.153 (“If the defendant does not produce enough evidence to support the claimed defense, a verdict is effectively directed in favor of the prosecution. . . . This is more troublesome, doctrinally. . . . Nevertheless, this practice will continue.”); Jeffries & Stephan, *supra* note 132, at 1347 n.62, 1348 (“There is no apparent reason to believe that the symbolic value of society’s commitment to proof beyond a reasonable doubt is in any way impaired by the existence of presumptions and affirmative defenses. These devices have existed for a long time and have not been widely perceived or popularly condemned as invasions of the presumption of innocence.”).

²¹⁴ *See, e.g.,* Gainey, 380 U.S. at 69–71 (rejecting arguments that a statutory presumption violated the defendant’s right to trial by jury and right against self-incrimination); *Yee Hem*, 268 U.S. at 185 (dismissing a challenge to a statutory presumption based on the privilege against self-incrimination); *Adams v. New York*, 192 U.S. 585, 598–99 (1904) (declining to consider the defendant’s argument that possession of gambling paraphernalia as prima facie evidence of knowing possession violated due process rights under the Fourteenth Amendment); *see also* Fuller & Urich, *supra* note 140, at 424 (“The fact remains, however, that [Justice Black’s objections in *Turner*] have been rarely expressly considered and never accepted by the Supreme Court. The only argument which has been subject to significant judicial consideration, that presumptive devices violate the protections against self-incrimination, is the argument most susceptible to dispute.”).

hibiting reallocation of the burden of proof would have equally undesirable effects upon criminal defendants.²¹⁵

Finally, the argument that presumptions and affirmative defenses unconstitutionally relieve the state from proving the defendant's guilt beyond a reasonable doubt is based on a formalistic interpretation of the criminal standard of proof and is not a concern in practice.²¹⁶ Burden shifting can lighten the evidentiary burden on the prosecution by permitting certain facts to be inferred from others for the purpose of a *prima facie* case.²¹⁷ Beyond this stage, however, the defendant has the opportunity to rebut the inferred fact, and the government once again bears the full burden of persuasion.²¹⁸ Presumptions are labor-saving devices, but their effect on litigation is limited to initial evidentiary burdens.²¹⁹ The ultimate decision of whether the state carried its burden of persuasion remains with the factfinder.²²⁰ Rather than depriving the accused of his or her constitutional rights, burden-shifting mechanisms actually benefit the defendant by providing a statutory defense, whether implicit (via presumptions and inferences) or explicit (via affirmative defenses), for individuals who fall within the scope of a criminal offense but whose conduct does not rise to a sufficient level of culpability.²²¹

C. *Burden-Shifting Devices in Current Cyberharassment Statutes*

As discussed in Part II.B, the majority of modern cyberharassment laws share common elements, but these statutory mechanisms implicitly favor one party above the other in litigation because they are couched in the perspective of either the victim or the harasser.²²² Specific intent and objective "reasonable victim" standards protect against overbreadth and unconstitutional vagueness, but they also weigh in favor of the defendant because they divert judicial focus away from the

²¹⁵ See Jeffries & Stephan, *supra* note 132, at 1358–59 (arguing that reallocation of the burden of proof is not related to the seriousness of criminal penalties and predicting that outlawing burden shifting devices would merely inhibit benevolent legislative reform).

²¹⁶ See Alexander, *supra* note 139, at 17–18; Harris, *supra* note 131, at 356–57.

²¹⁷ See Alexander, *supra* note 139, at 17–18.

²¹⁸ See *id.* at 18 (“[The plaintiff] may struggle as best he can to reach the haven of the *prima facie* case; he may ‘hitch-hike’ part of the way upon a passing presumption. Once he reaches this battle area, however, he should be compelled to fight it out with the only weapons which persuasion allows.”).

²¹⁹ See *id.* at 17–18.

²²⁰ See *id.*

²²¹ See Fuller & Urich, *supra* note 140, at 429.

²²² See Goodno, *supra* note 1, at 134, 139; Lamplugh & Infield, *supra* note 77, at 865; Merschman, *supra* note 13, at 268–69; *supra* notes 88–126 and accompanying text.

victim's personal response to the harassment and impose heavy evidentiary burdens upon the government.²²³ In contrast, subjective "reasonable victim" or "reasonable harasser" standards favor the victim by focusing primarily on the reasonableness of the offender's actions, rather than the sensitivity of the victim, and by ensuring that the trier of fact considers each offense on an individual basis.²²⁴ Statutes featuring subjective elements risk being invalidated as unconstitutionally vague, however, due to their reliance on the varying and unpredictable mental states of the parties involved.²²⁵ Because of their ability to balance the interests of both parties, burden-shifting devices should compensate for the shortcomings of these statutory strategies.²²⁶ This Section identifies promising models for states to emulate; specifically, the United Kingdom and several U.S. states have already incorporated affirmative defenses and presumptions into their cyberharassment statutes, and these statutes have successfully withstood constitutional challenge.²²⁷

1. Affirmative Defenses in Practice

One example of affirmative defenses can be seen in the United Kingdom's Protection from Harassment Act of 1997 (PHA).²²⁸ Section 4 of the Act imposes criminal penalties upon individuals whose course of conduct places others in fear of violence on more than two occasions and employs a reasonableness standard from the perspective of the harasser.²²⁹ Additionally, section 4 contains a burden-shifting device that allows the defendant to show evidence pursuant to three affirmative defenses, including whether his or her conduct was reasonable for pro-

²²³ See Lamplugh & Infield, *supra* note 77, at 863, 865; Merschman, *supra* note 13, at 269; Radosevich, *supra* note 33, at 1384.

²²⁴ See Merschman, *supra* note 13, at 270, 287.

²²⁵ See Lamplugh & Infield, *supra* note 77, at 865; Volokh, *supra* note 12, at 421; Barton, *supra* note 81, at 481–82.

²²⁶ See Alexander, *supra* note 139, at 2; Chamberlain, *supra* note 167, at 287–88.

²²⁷ See KAN. STAT. ANN. § 21-3438 (2007 & Supp. 2009); MICH. COMP. LAWS ANN. §§ 750.411h, .411i (West 2004); MONT. CODE ANN. §§ 45-8-213, § 45-5-220 (2009); N.H. REV. STAT. ANN. § 633:3-a (2007); OKLA. STAT. tit. 21 § 1173 (2002); TENN. CODE ANN. § 39-17-315 (2010); VT. STAT. ANN. tit. 13, § 1027 (2009); WASH. REV. CODE ANN. § 9A.46.110 (West 2009); Protection from Harassment Act, 1997, 25 & 26 Eliz. 2, c. 40 (Eng.); *infra* notes 228–257 and accompanying text.

²²⁸ See Protection from Harassment Act, 1997, 25 & 26 Eliz. 2, c. 40 (Eng.).

²²⁹ *Id.* § 4(2) (“[The] person whose course of conduct is in question ought to know that it will cause another to fear that violence will be used against him on any occasion if a reasonable person in possession of the same information would think the course of conduct would cause the other to so fear on that occasion.”).

tecting himself or another, or the property thereof.²³⁰ The British Parliament originally enacted the PHA to redress traditional forms of stalking and to resolve doctrinal inconsistencies in the common law; the statute's language, however, is sufficiently broad to encompass many types of harassment, both civil and criminal.²³¹

Affirmative defenses are rarely explicitly included in U.S. cyberharassment law, although states like New Hampshire have employed statutory language excepting "constitutionally protected" or otherwise lawful activity that could be construed as a defense for which the accused would bear the burden of proof.²³² Additionally, a few states, such as Utah, explicitly preclude the defendant from asserting certain

²³⁰ *Id.* § 4(3). Section 4(3) of the PHA provides:

It is a defense for a person charged with an offence under this section to show that—

- (a) his course of conduct was pursued for the purpose of preventing or detecting crime,
- (b) his course of conduct was pursued under any enactment or rule of law or to comply with any condition or requirement imposed by any person under any enactment, or
- (c) the pursuit of his course of conduct was reasonable for the protection of himself or another or for the protection of his or another's property.

Id. The prosecution is not obligated to affirmatively prove that the defendant's conduct is unreasonable before the defendant can invoke the affirmative defense. *See* Lamplugh & Infield, *supra* note 77, at 864.

²³¹ Susan Harthill, *Bullying in the Workplace: Lessons from the United Kingdom*, MINN. J. INT'L L. 247, 274 (2008) (explaining that the PHA has been drafted broadly enough to encompass harassment in the workplace, racial harassment, domestic violence, and even civil protests). In fact, the statute never conclusively defines the term "harassment," merely including acts like "alarming" or "causing . . . distress" within its ambit. *See* PHA § 7(2). This broad statutory construction, as well as the PHA's primary emphasis on psychological harm as opposed to physical harm or bodily injury, sets this statute apart from most legislation in the United States. Harthill, *supra*, at 294.

²³² *See* State v. Pierce, 887 A.2d 132, 135 (N.H. 2005) (invalidating subdivision 1(f) of New Hampshire's harassment statute and determining that, even if the statutory exception for lawful communication or constitutionally protected activity constituted an affirmative defense, the statute remained overbroad). In the majority of states with cyberharassment laws that exclude constitutionally protected activity, however, the exception does not affect the burden of proof and is not crucial to the validity of the statute. *See, e.g.,* State v. Cardell, 723 A.2d 111, 114 (N.J. Super. Ct. App. Div. 1999) (quoting McDade v. State, 693 A.2d 1062, 1065 (Del. 1997)) ("That vaguely expressed exception from the original statute's reach added nothing of substance. . . . Anyone exercising First Amendment rights . . . cannot be convicted under the statute 'even without any specific exception.'"); State v. Ruesch, 571 N.W.2d 898, 901–02 (Wis. Ct. App. 1997) ("Because [the exception] provides no elements of the crime of stalking, it plays no role in the State's burden of proof at trial.").

defenses like lack of notice or specific intent to cause fear or emotional distress.²³³

2. Presumptions and Inferences in Practice

No U.S. federal legislation that applies to cyberharassment features a burden-shifting device in the context of criminal law.²³⁴ U.S. state statutes, however, tend to include nonmandatory presumptions and inferences rather than affirmative defenses.²³⁵ Cyberharassment laws in Kansas, Michigan, Montana, New Hampshire, Oklahoma, Tennessee, Vermont, and Washington, upon the establishment of certain facts or prima facie evidence, permit the factfinder to presume some element of the offense, such as mens rea, specific intent, or actual infliction of harassment or fear upon the victim.²³⁶ For example, Michigan's stalking law permits the trier of fact to presume the defendant's conduct caused the victim to feel frightened, intimidated, or harassed where the prosecution presents evidence that the defendant continued to engage in unconsented contact with the victim after being requested by the victim to stop.²³⁷ Washington's stalking statute similarly provides that any attempt to contact or follow the victim, after receiving actual notice that such contact is unwanted, serves as prima facie evidence of the defendant's intent to intimidate or harass the victim.²³⁸

Of the seven states that employ burden-shifting devices, all characterize the device as a presumption except for Vermont's "disturbing the peace" statute, which provides for a permissible inference of intent to

²³³ See UTAH CODE ANN. § 76-5-106.5(4) (LexisNexis 2008) ("In any prosecution under this section, it is not a defense that the actor: (a) was not given actual notice that the course of conduct was unwanted; or (b) did not intend to cause the victim fear or other emotional distress.").

²³⁴ See Interstate Communications Act, 18 U.S.C. § 875(c) (2006); Interstate Stalking and Prevention Act, 18 U.S.C. § 2261A (2006); Communications Decency Act, 47 U.S.C. § 223 (2006). The CDA includes affirmative defenses for ISPs and employers, but these defenses are only applicable to civil liability and are not available for defendants who actually initiate or engage in the disputed communications. See 47 U.S.C. § 223(b)(3), (e).

²³⁵ See KAN. STAT. ANN. § 21-3438 (2007 & Supp. 2009); MICH. COMP. LAWS ANN. §§ 750.411h, .411i (West 2004); MONT. CODE ANN. §§ 45-8-213, 45-5-220 (2009); N.H. REV. STAT. ANN. § 633:3-a (2007); OKLA. STAT. tit. 21 § 1173 (2002); TENN. CODE ANN. § 39-17-315 (2010); VT. STAT. ANN. tit. 13, § 1027 (2009); WASH. REV. CODE ANN. § 9A.46.110 (West 2009); Protection from Harassment Act, 1997, 25 & 26 Eliz. 2, c. 40 (Eng.).

²³⁶ See KAN. STAT. ANN. § 21-3438; MICH. COMP. LAWS ANN. §§ 750.411h, .411i; MONT. CODE ANN. §§ 45-8-213, § 45-5-220; N.H. REV. STAT. ANN. § 633:3-a; OKLA. STAT. tit. 21 § 1173; TENN. CODE ANN. § 39-17-315; VT. STAT. ANN. tit. 13, § 1027; WASH. REV. CODE ANN. § 9A.46.110; Protection from Harassment Act, 1997, 25 & 26 Eliz. 2, c. 40 (Eng.).

²³⁷ MICH. COMP. LAWS ANN. § 750.411h.

²³⁸ WASH. REV. CODE ANN. § 9A.46.110.

terrify, threaten, harass, or annoy from the defendant's use of obscene, lewd, or lascivious language, threats, or repeated anonymous electronic communications.²³⁹ Only Kansas and New Hampshire's stalking statutes involve presumptions without indication that the presumption is rebuttable or provides for only prima facie evidence.²⁴⁰

Burden-shifting mechanisms that have been introduced into U.S. cyberharassment laws have yet to be successfully challenged on free speech or due process grounds.²⁴¹ In order to preserve this trend, an ideal statutory formulation for criminal cyberharassment statutes would involve a combination of conventional elements, the aggregate effect of which would account for the perspectives of both the victim and the alleged harasser.²⁴² For example, one embodiment could include: a specific intent element paired with an objective "reasonable victim" standard; an explicit exception for constitutionally protected activity, which could either function as clarification of the offense or an affirmative defense; and finally a burden-shifting device, embodied as either an implied affirmative defense or a nonmandatory presumption.²⁴³ If a presumption is employed, the statute should make clear that the presumption is noncompulsory, rebuttable, and provides only for prima facie evidence of the relevant element of the offense, in order to avoid raising constitutional issues from *Mullaney* and *Sandstrom*.²⁴⁴

Oklahoma's stalking statute provides an excellent example of a cyberharassment law that has effectively supplemented conventional statutory elements—in this case, an objective "reasonable victim" standard, an implied specific intent element, and an exception for constitu-

²³⁹ See VT. STAT. ANN. tit. 13, § 1027.

²⁴⁰ See KAN. STAT. ANN. § 21-3438; N.H. REV. STAT. ANN. § 633:3-a.

²⁴¹ See *Staley v. Jones*, 108 F. Supp. 2d 777, 780 (W.D. Mich. 2000) (ruling that Michigan's aggravated stalking statute does not unconstitutionally shift the burden of proof to the defendant), *rev'd on other grounds*, 239 F.3d 739 (6th Cir. 2001); *People v. White*, 536 N.W.2d 876, 884–85 (Mich. Ct. App. 1995) (upholding the rebuttable presumption in Michigan's aggravated stalking statute); *State v. Saunders*, 886 P.2d 496, 497–98 (Okla. 1994) (ruling that Oklahoma's stalking statute does not unconstitutionally shift the burden of proof to the defendant). As previously discussed in Part IV.A, in order for a presumption to be constitutional, it cannot shift the burden of persuasion, must be nonmandatory, and should satisfy the current version of the U.S. Supreme Court's rational connection test as set forth in *Leary*, taking into account any substantial inconvenience to the prosecution to prove the presumed fact under *Morrison*'s comparative convenience test. See *Leary*, 219 U.S. at 36; *Morrison*, 395 U.S. at 88–91.

²⁴² See OKLA. STAT. tit. 21, § 1173.

²⁴³ See *Pierce*, 887 A.2d at 135.

²⁴⁴ See *Sandstrom*, 442 U.S. at 521–23; *Mullaney*, 421 U.S. at 703.

tionally protected activities—with a burden-shifting device.²⁴⁵ Under the statute, if the prosecution provides evidence that the defendant continued to engage in unconsented contact with the victim after being requested by the victim to stop, such conduct gives rise to a rebuttable presumption that the defendant's actions resulted in impact or harm upon the victim.²⁴⁶ This presumption works in conjunction with the statute's other elements by allowing one requirement of the offense (harm to the victim) to be inferred by *prima facie* evidence of culpable behavior within the scope of the statute (repeated following or harassment).²⁴⁷ The statute, however, provides the accused with opportunities for exculpation, either by showing that a reasonable person would not have been threatened by his or her behavior via the objective "reasonable victim" standard, demonstrating that the disputed conduct fell within the protection of the Constitution or served a legitimate purpose, or by rebutting the presumption that the victim actually felt frightened or harassed.²⁴⁸

Several aspects of the Oklahoma statute ensure that it strikes the proper balance between efficacy and the defendant's constitutional rights, making it an ideal model.²⁴⁹ The specific intent element targets only purposeful, culpable behavior deserving of criminal sanctions and protects the statute from First Amendment challenges.²⁵⁰ The objective "reasonable victim" element likewise avoids an overly subjective standard that might lead to invalidation for unconstitutional vagueness or overbreadth.²⁵¹ The statutory language specifically describes the burden-shifting mechanism as a "rebuttable presumption," ensuring that it cannot be struck down as unconstitutional for impermissibly shifting

²⁴⁵ See OKLA. STAT. tit. 21, § 1173; *Saunders*, 886 P.2d at 497 (reading a specific intent element into the Oklahoma stalking statute and determining that the word "repeatedly" elucidates that intent).

²⁴⁶ See OKLA. STAT. tit. 21, § 1173. The relevant statutory language reads:

Evidence that the defendant continued to engage in a course of conduct involving repeated unconsented contact . . . with the victim after having been requested by the victim to discontinue the same or any other form of unconsented contact, and to refrain from any further unconsented contact with the victim, shall give rise to a rebuttable presumption that the continuation of the course of conduct caused the victim to feel terrorized, frightened, intimidated, threatened, harassed, or molested.

Id.

²⁴⁷ See *id.*

²⁴⁸ See *id.* § 1173(A)(1), (E), (F)(1).

²⁴⁹ See *id.* § 1173(E), (F).

²⁵⁰ See Barton, *supra* note 81, at 481.

²⁵¹ See Volokh, *supra* note 12, at 421; Barton, *supra* note 81, at 481–82.

the burden of persuasion under *Mullaney* or imposing a conclusive or mandatory presumption.²⁵² Additionally, the statute provides concrete examples of “unconsented contact” that could awaken the presumption, thereby notifying potential offenders and lessening the risk of invalidation under the void-for-vagueness doctrine.²⁵³

In 1994, the Court of Criminal Appeals of Oklahoma upheld the burden-shifting element of the stalking statute against challenges of overbreadth and vagueness in *State v. Saunders*.²⁵⁴ Applying the rational connection test, the court ruled that the rebuttable presumption of harm did not unconstitutionally shift the burden of proof to the defendant because there was a rational connection between the facts proven (the continuation of unconsented contact by the accused) and the fact presumed (the victim actually feeling frightened or harassed).²⁵⁵ The court also defended the stalking statute against allegations of vagueness under the Due Process Clause, ruling that its language gave clear and fair notice of the proscribed activity and acknowledging that “[a] careful balance must be achieved for a statute addressing stalking to be effective. Stalking statutes must be defined as broadly as possible to maximize victim protection, but narrowly enough to prevent serious abuse.”²⁵⁶ Similarly worded statutes featuring rebuttable presumptions, such as Michigan’s, have likewise withstood constitutional attacks, indicating that burden-shifting devices hold substantial promise for balancing the constitutional rights and safety concerns of online speakers and cyberharassment victims.²⁵⁷

CONCLUSION

Cyberharassment statutes that incorporate burden-shifting devices have the potential to account for inherent disparities between cyberharassers and their victims, where the details of the crime are difficult for the state to discover and are typically within only the defendant’s knowledge. Although burden shifting is normally considered prosecu-

²⁵² See *Sandstrom*, 442 U.S. at 521–23; *U.S. Gypsum Co.*, 438 U.S. at 446; *Mullaney*, 421 U.S. at 703; *Morissette*, 342 U.S. at 275.

²⁵³ See OKLA. STAT. tit. 21, § 1173(F)(4).

²⁵⁴ 886 P.2d at 497–98.

²⁵⁵ *Id.*

²⁵⁶ *Id.* at 497.

²⁵⁷ See *Staley*, 108 F. Supp. 2d at 780 (ruling that the rebuttable presumption featured in Michigan’s aggravated stalking statute did not unconstitutionally shift the burden of proof to the accused); *White*, 536 N.W.2d at 885 (upholding the rebuttable presumption in Michigan’s stalking statute and determining that the ultimate burden of proof for every element of the offense remained with the prosecution).

tion-oriented, affirmative defenses and rebuttable presumptions can function as additional tools for cyberharassment victims and the state in a relatively new area of the criminal law, where defendants can easily conceal their identities from victims, law enforcement, and even ISPs, and elicit evidence relevant to the offense that the accused is in the best position to provide. Inferences created by these devices are nonmandatory and thus safely within constitutional bounds; the factfinder may accept them only when it is properly persuaded that they are true. Finally, burden shifting increases fundamental fairness for both parties, not only aiding the prosecution, but also creating additional avenues of exculpation for nonculpable defendants. Affirmative defenses and presumptions should therefore be considered legitimate statutory strategies, supplementing specific intent and standards of reasonableness, for establishing a balance of convenience for both the victim and the accused in future state and federal cyberharassment laws.

AIMEE FUKUCHI

APPENDIX OF CURRENT STATE AND FEDERAL CYBERHARASSMENT
STATUTES²⁵⁸

Current State and Federal Cyberharassment Statutes		
Federal/State	Statute	Elements
Federal	Interstate Communications Act, 18 U.S.C. § 875(c) (2006).	(none)
	Interstate Stalking Punishment and Prevention Act, 18 U.S.C. § 2261A (2006).	1) Specific intent; 2) Objective reasonableness standard based on victim.
	Communications Decency Act, 47 U.S.C. § 223 (2006).	1) Specific intent; 2) Affirmative defenses (available under section 223(c), primarily for ISPs and employers).
Alabama	ALA. CODE § 13A-11-8 (LexisNexis 2005). Harassment or harassing communications.	1) Specific intent; 2) Reasonableness standard, perspective unclear (“in a manner likely to harass or cause alarm”).
Alaska	ALASKA STAT. § 11.41.270 (2008). Stalking in the second degree.	1) Objective reasonableness standard based on victim (imputed from case law: <i>Cooper v. Cooper</i> , 144 P.3d 451, 456 (Alaska 2006); <i>Cook v. State</i> , 36 P.3d 710, 718–19 (Alaska Ct. App. 2001)).
	ALASKA STAT. § 11.61.120 (2008). Harassment in the second degree.	1) Specific intent.
Arizona	ARIZ. REV. STAT. ANN. § 13-2921 (2010). Harassment; classification; definition.	1) Specific intent; 2) Objective reasonableness standard based on victim; 3) Exception for constitutionally protected speech.
Arkansas	ARK. CODE ANN. § 5-41-108 (2006). Unlawful computerized communications.	1) Specific intent.
	ARK. CODE ANN. § 5-27-306 (2006). Internet stalking of a child.	(none)
California	CAL. PENAL CODE § 422 (West 2010). Elements of offense; punishment; “immediate family” defined.	1) Specific intent; 2) Objective reasonableness standard based on victim.
	CAL. PENAL CODE § 646.9 (West 2010). Stalking.	1) Specific intent; 2) Objective reasonableness standard based on victim; 3) Exception for constitutionally protected speech.
	CAL. PENAL CODE § 653m (West 2010). Telephone calls or contact by electronic communication device	1) Specific intent.

²⁵⁸ Italicized text denotes burden-shifting elements.

	with intent to annoy.	
Colorado	COLO. REV. STAT. § 18-9-111 (2010). Harassment.	1) Specific intent; 2) Reasonableness standard, perspective unclear (“in a manner likely to provoke a violent or disorderly response”).
Connecticut	CONN. GEN. STAT. ANN. § 53a-182b (West 2007). Harassment in the first degree: Class D felony.	1) Specific intent; 2) Reasonableness standard, perspective unclear (“in a manner likely to cause annoyance or alarm”).
	CONN. GEN. STAT. ANN. § 53a-183 (West 2007). Harassment in the second degree: Class C misdemeanor.	1) Specific intent; 2) Reasonableness standard, perspective unclear (“in a manner likely to cause annoyance or alarm”).
Delaware	DEL. CODE ANN. tit. 11, § 1311 (2007 & Supp. 2010). Harassment; class A misdemeanor.	1) Specific intent; 2) Objective reasonableness standard based on victim. 3) Objective reasonableness standard based on harasser.
District of Columbia	(none)	(none)
Florida	FLA. STAT. ANN. § 817.568 (West 2006). Criminal use of personal identification information.	1) Specific intent; 2) Exception for constitutionally protected speech.
	FLA. STAT. ANN. § 784.048 (West 2007 & Supp. 2010). Stalking; definitions; penalties.	1) Specific intent; 2) Objective reasonableness standard based on victim; 3) Exception for constitutionally protected speech.
Georgia	GEORGIA CODE ANN. § 16-5-90 (2007). Stalking.	1) Specific intent; 2) Objective reasonableness standard based on victim.
Hawaii	HAW. REV. STAT. ANN. § 711-1106 (LexisNexis 2007 & Supp. 2009). Harassment.	1) Specific intent; 2) Objective reasonableness standard based on victim.
	HAW. REV. STAT. ANN. § 711-1106.5 (LexisNexis 2007 & Supp. 2009). Harassment by stalking.	1) Specific intent.
Idaho	IDAHO CODE ANN. § 18-7906 (2004). Stalking in the second degree.	1) Objective reasonableness standard based on victim; 2) Exception for constitutionally protected speech.
Illinois	720 ILL. COMP. STAT. ANN. 5/12-7.5 (West 2002 & Supp. 2010). Cyberstalking.	1) Objective reasonableness standard based on victim; 2) Objective reasonableness standard based on harasser.
	720 ILL. COMP. STAT. ANN. 135/1-2 (West 2010). Harassment through electronic communications.	1) Specific intent.
Indiana	IND. CODE ANN. § 35-45-2-2 (LexisNexis 2009). Harassment; “obscene message” defined.	1) Specific intent; 2) Objective reasonableness standard based on victim (imputed from case law: <i>Leuteritz v. State</i> , 534 N.E.2d

		265, 266–67 (Ind. Ct. App. 1989) (quoting <i>Kinney v. State</i> , 404 N.E.2d 49 (Ind. Ct. App. 1980)) (emphasizing an objective, rather than subjective viewpoint)].
Iowa	IOWA CODE ANN. § 708.7 (West 2003 & Supp. 2010). Harassment.	1) Specific intent; 2) Reasonableness standard, perspective unclear (“in a manner likely to cause the other person annoyance or harm”).
Kansas	KAN. STAT. ANN. § 21-3438 (2007 & Supp. 2009). Stalking.	1) Objective reasonableness standard based on victim; 2) <i>Presumption that the defendant acted intentionally for any future act, after being served with a protective order or continuing to engage in stalking after being advised by a law enforcement officer;</i> 3) Exception for constitutionally protected speech.
Kentucky	KY. REV. STAT. ANN. § 508.130 (LexisNexis 2008 & Supp. 2009). Definitions for KRS 508.130 to 508.150.	1) Objective reasonableness standard based on victim; 2) Exception for constitutionally protected speech.
Louisiana	LA. REV. STAT. ANN. § 14:40.2 (West, Westlaw through 2007 Sess.). Stalking.	1) Specific intent; 2) Objective reasonableness standard based on victim; 3) Exception for constitutionally protected speech.
	LA. REV. STAT. ANN. § 14:40.3 (West, Westlaw through 2007 Sess.). Cyberstalking.	1) Specific intent; 2) Exception for constitutionally protected speech.
Maine	ME. REV. STAT. ANN. tit. 17A, § 210-A (2006 & Supp. 2009). Stalking.	1) Objective reasonableness standard based on victim.
Maryland	MD. CODE ANN., CRIM. LAW § 3-805 (LexisNexis 2002). Misuse of electronic mail.	1) Specific intent; 2) Exception for constitutionally protected speech.
Massachusetts	MASS. GEN. LAWS ch. 265, § 43 (2008). Stalking; punishment.	1) Specific intent; 2) Objective reasonableness standard based on victim.
	MASS. GEN. LAWS ch. 265, § 43A (2008). Criminal harassment; punishment.	1) Objective reasonableness standard based on victim.
Michigan	MICH. COMP. LAWS ANN. § 750.411h (West 2004). Stalking; definitions; violation, penalties; probation, term, conditions; evidence, rebuttable presumption; penalty additional.	1) Objective reasonableness standard based on victim; 2) <i>Rebuttable presumption that defendant’s continuation of unconsented contact, after being requested by the victim to stop, caused the victim to feel terrorized, frightened, intimidated, threatened, harassed, or molested;</i> 3) Exception for constitutionally protected speech.
	MICH. COMP. LAWS ANN. § 750.411i	1) Objective reasonableness standard

	(West 2004). Aggravated stalking; course of conduct; violation, penalties; probation; rebuttable presumption.	based on victim; 2) <i>Rebuttable presumption that defendant's continuation of unconsented contact, after being requested by the victim to stop, caused the victim to feel terrorized, frightened, intimidated, threatened, harassed, or molested;</i> 3) Exception for constitutionally protected speech.
	MICH. COMP. LAWS ANN. § 750.411s (West 2004). Posting messages through electronic medium without consent.	1) Specific intent; 2) Objective reasonableness standard based on victim; 3) Objective reasonableness standard based on harasser; 4) Exception for constitutionally protected speech.
Minnesota	MINN. STAT. ANN. § 609.749 (West 2009). Harassment; stalking; penalties.	1) Objective reasonableness standard based on harasser (explicit statement that no proof of specific intent is required); 2) Exception for constitutionally protected speech.
Mississippi	MISS. CODE ANN. § 97-29-45 (2006). Obscene electronic communications.	1) Specific intent.
	MISS. CODE ANN. § 97-45-15 (2006). "Cyberstalking"; penalties.	1) Specific intent; 2) Exception for constitutionally protected speech.
Missouri	MO. REV. STAT. § 565.225 (1999 & Supp. 2010). Crime of stalking—definitions—penalties.	1) Specific intent; 2) Objective reasonableness standard based on victim; 3) Exception for constitutionally protected speech.
	MO. REV. STAT. § 565.090 (1999 & Supp. 2010). Harassment.	1) Specific intent; 2) Objective reasonableness standard based on victim.
Montana	MONT. CODE ANN. § 45-8-213 (2009). Privacy in communications.	1) Specific intent; 2) <i>Rebuttable presumption that defendant's use of lewd or obscene language, threats, or lewd and lascivious suggestions constitutes prima facie evidence of intent to terrify, intimidate, threaten, harass, annoy, or offend.</i>
	MONT. CODE ANN. § 45-5-220 (2009). Stalking—exemption—penalty.	1) <i>Attempts to contact the victim after actual notice that contact is unwanted constitutes prima facie evidence of purposeful or knowing harassment of the victim;</i> 2) Objective reasonableness standard based on victim; 3) Exception for constitutionally protected speech.
Nebraska	(none)	(none)
Nevada	NEV. REV. STAT. ANN. § 200.575	1) Specific intent;

	(LexisNexis 2006 & Supp. 2009). Stalking: Definitions; penalties.	2) Objective reasonableness standard based on victim; 3) Exception for constitutionally protected speech.
New Hampshire	N.H. REV. STAT. ANN. § 644:4 (2007 & Supp. 2009). Harassment.	1) Specific intent. Provision containing possible affirmative defense for constitutionally protected conduct or communication with a lawful purpose (section (1)(f)) held unconstitutional in <i>State v. Pierce</i> , 887 A.2d 132, 135 (N.H. 2005), unrelated to the existence of the defense.
	N.H. REV. STAT. ANN. § 633:3-a (2007). Stalking.	1) Objective reasonableness standard based on victim; 2) Objective reasonableness standard based on harasser; 3) <i>Presumption of knowledge after being advised by law enforcement officer or served with a protective order</i> ; 4) Exception for conduct “necessary to accomplish a legitimate purpose independent of making contact with the targeted person.” 5) Exception for constitutionally protected speech.
New Jersey	N.J. STAT. ANN. § 2C:12-10 (West 2005 & Supp. 2010). Stalking.	1) Objective reasonableness standard based on victim; 2) Exception for constitutionally protected speech.
New Mexico	(none)	(none)
New York	N.Y. PENAL LAW § 240.30 (McKinney 2008). Aggravated harassment in the second degree.	1) Specific intent; 2) Reasonableness standard, perspective unclear (“in a manner likely to cause annoyance or alarm”).
North Carolina	N.C. GEN. STAT. § 14-196 (2009). Using profane, indecent or threatening language to any person over telephone; annoying or harassing by repeated telephoning or making false statements over telephone.	1) Specific intent.
	N.C. GEN. STAT. § 14-196.3 (2009). Cyberstalking.	1) Specific intent; 2) Exception for constitutionally protected speech.
North Dakota	N.D. CENT. CODE § 12.1-17-07 (1997 & Supp. 2009). Harassment.	1) Specific intent.
Ohio	OHIO REV. CODE ANN. § 2903.211 (West 2006 & Supp. 2010). Menacing by stalking.	1) Objective reasonableness standard based on victim.
	OHIO REV. CODE ANN. § 2917.21 (West 2006). Telecommunications harassment.	1) Specific intent.

Oklahoma	OKLA. STAT. tit. 21, § 1173 (2002). Stalking—Penalties.	1) Specific intent (imputed from case law. <i>State v. Saunders</i> , 886 P.2d 496, 497 (Okla. Crim. App. 1994)). 2) Objective reasonableness standard based on victim; 3) <i>Rebuttable presumption that defendant's continuation of course of conduct, after being requested by the victim to stop, caused the victim to feel terrorized, frightened, intimidated, threatened, harassed, or molested</i> ; 4) Exception for constitutionally protected speech.
Oregon	OR. REV. STAT. § 163.732 (2009). Stalking.	1) Objective reasonableness standard based on victim.
	OR. REV. STAT. § 166.065 (2009). Harassment.	1) Reasonableness standard, perspective unclear (“which report/threat reasonably would be expected to cause alarm”); 2) Objective reasonableness standard based on harasser (section (1)(a)(B)) held unconstitutional in <i>State v. Johnson</i> , 191 P.3d 665, 669 (Or. 2008).
Pennsylvania	18 PA. CONS. STAT. ANN. § 2709 (West 2000 & Supp. 2010). Harassment.	1) Specific intent.
	18 PA. CONS. STAT. ANN. § 2709.1 (West 2000 & Supp. 2010). Stalking.	1) Specific intent; 2) Reasonableness based on victim.
Rhode Island	R.I. GEN. LAWS § 11-52-4.2 (West, Westlaw through 2008 Sess.). Cyberstalking and cyberharassment prohibited.	1) Specific intent (“for the sole purpose of harassing that person”); 2) Objective reasonableness standard based on victim; 3) Exception for constitutionally protected speech.
South Carolina	S.C. CODE ANN. § 16-3-1700(A) (2003 & Supp. 2009). Definitions. (Harassment in the first degree)	1) Objective reasonableness standard based on victim; 2) Exception for constitutionally protected speech.
	S.C. CODE ANN. § 16-3-1700(B) (2003 & Supp. 2009). Definitions. (Harassment in the second degree)	1) Objective reasonableness standard based on victim; 2) Exception for constitutionally protected speech.
	S.C. CODE ANN. § 16-3-1700(C) (2003 & Supp. 2009). Definitions. (Stalking)	1) Specific intent; 2) Objective reasonableness standard based on victim; 3) Exception for constitutionally protected speech.
South Dakota	S.D. CODIFIED LAWS § 22-19A-1 (2004 & Supp. 2010). Stalking as a misdemeanor—Second offense a felony.	1) Specific intent; 2) Objective reasonableness standard based on victim.
	S.D. CODIFIED LAWS § 49-31-31 (2004 & Supp. 2010). Threatening	1) Specific intent.

	or harassing contacts by telephone or other electronic communication device as misdemeanor.	
Tennessee	TENN. CODE ANN. § 39-17-308 (2010). Harassment.	1) Specific intent; 2) Objective reasonableness standard based on victim; 3) Objective reasonableness standard based on harasser.
	TENN. CODE ANN. § 39-17-315 (2010). Stalking, aggravated stalking, and especially aggravated stalking.	1) Objective reasonableness standard based on victim; 2) <i>Rebuttable presumption that that defendant's continuation of contact, after being requested by the victim to stop, constitutes prima facie evidence that the conduct caused the victim to feel terrorized, frightened, intimidated, threatened, harassed, or molested;</i> 3) Exception for constitutionally protected speech
Texas	TEX. PENAL CODE ANN. § 42.07 (Vernon 2003 & Supp. 2010). Harassment.	1) Specific intent Subjective reasonableness standard based on victim (section (a) (7)) held unconstitutional in <i>Karenev v. State</i> , 258 S.W.3d 210, 214, 217 (Tex. App. 2008), rev'd on other grounds, 281 S.W.3d 428 (Tex. Crim. App. 2009).
Utah	UTAH CODE ANN. § 76-5-106.5 (LexisNexis 2008). Stalking—Definitions—Injunction—Penalties.	1) Objective reasonableness standard based on victim; 2) Objective reasonableness standard based on harasser.
Vermont	VT. STAT. ANN. tit. 13, § 1027 (2009). Disturbing peace by use of telephone or other electronic communications.	1) Specific intent; 2) <i>Inference of intent from use of lewd, lascivious or indecent language or repeated anonymous communications.</i>
	VT. STAT. ANN. tit. 13, § 1061 (2009). Definitions.	1) Objective reasonableness standard based on victim; 2) Exception for constitutionally protected speech.
Virginia	VA. CODE ANN. § 18.2-60 (2009). Threats of death or bodily injury to a person or member of his family; threats to commit serious bodily harm to persons on school property; penalty.	1) Specific intent.
	VA. CODE ANN. § 18.2-152.7:1 (2009). Harassment by computer; penalty.	1) Specific intent.
Washington	WASH. REV. CODE ANN. § 9A.46.020 (West 2009). Definition—Penalties.	1) Objective reasonableness standard based on victim. Subjective reasonableness standard based on victim (section (1) (a) (iv)) held unconstitutional in <i>State v. Williams</i> , 26 P.3d 890, 895 (Wash.

		2001).
	WASH. REV. CODE ANN. § 9A.46.110 (West 2009). Stalking.	1) Specific intent; 2) Objective reasonableness standard based on victim; 3) Objective reasonableness standard based on harasser; 4) <i>Rebuttable presumption that defendant's continuation of unwanted contact or following constitutes prima facie evidence of defendant's intent to harass or intimidate.</i>
	WASH. REV. CODE ANN. § 9.61.260 (West 2010). Cyberstalking.	1) Specific intent.
	WASH. REV. CODE ANN. § 10.14.020 (West 2002). Definitions.	1) Objective reasonableness standard based on victim; 2) Exception for constitutionally protected speech.
West Virginia	W. VA. CODE ANN. § 61-3C-14a (LexisNexis 2010). Obscene, anonymous, harassing and threatening communications by computer; penalty.	1) Specific intent; 2) Objective reasonableness standard based on victim.
Wisconsin	Wis. STAT. ANN. § 947.0125 (West 2005). Unlawful use of computerized communication systems.	1) Specific intent.
	Wis. STAT. ANN. § 940.32 (West, Westlaw through 2005–2006 Sess.). Stalking.	1) Objective reasonableness standard based on victim; 2) Objective reasonableness standard based on harasser; 3) Exception for constitutionally protected speech.
Wyoming	WYO. STAT. ANN. § 6-2-506 (2009). Stalking; penalty.	1) Specific intent; 2) Objective reasonableness standard based on victim; 3) Objective reasonableness standard based on harasser; 4) Exception for constitutionally protected speech.