CUTTING CYBERSTALKING'S GORDIAN KNOT: A SIMPLE AND UNIFIED STATUTORY APPROACH

Casey O'Connor[*]

I. INTRODUCTION

> The Internet and other telecommunications technologies are promoting advances in virtually every aspect of society and every corner of the globe: fostering commerce, improving education and health care, promoting participatory democracy in the United States and abroad, and facilitating communications among family and friends, whether across the street or around the world. Unfortunately, many of the attributes of this technology—low cost, ease of use, and anonymous nature, among others—make it an attractive medium for fraudulent scams, child sexual exploitation, and increasingly, a new concern known as "cyberstalking."[1]

These words, written more than a decade ago, described the emerging difficulty of keeping apace with technology in a rapidly changing world. With the explosion of social media and expansion in online capabilities forming new means through which cyberstalkers accomplish their malicious ends, these concerns resonate no less strongly today. Although the law has attempted to keep up, the current system creates dueling obligations and confusions that often obscure justice.

Consider the case of Jake Baker and Arthur Gonda.[2] The two men were online acquaintances who exchanged e-mails that expressed their mutual "sexual interest in violence against women."[3] Their often-explicit communications detailed their intention to

[*] J.D. Candidate, 2013, Seton Hall University School of Law; B.A., *summa cum laude*, 2009, Rutgers University. The author thanks Professor Kip Cornwell for his guidance.

[1] 1999 REPORT ON CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY: A REPORT FROM THE ATTORNEY GENERAL TO THE VICE PRESIDENT (Aug. 1999), *available at* http://www.cyber-rights.org/documents/cyberstalkingreport.htm.

[2] United States v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997).

[3] *Id.* at 1493.

convert their interest into action.[4] For example, "Wiat [sic] until late at night. grab [sic] her when she goes to unlock the door. Knock her unconscious. and [sic] put her into one of those portable lockers (forget the word for it). or [sic] even a duffle bag. Then hurry her out to the car and take her away . . . What do you think?"[5] Baker went further, posting a story on an online forum that described "the torture, rape, and murder of a young woman who shared the name of one of Baker's classmates at the University of Michigan."[6] When the story was discovered, the duo was indicted under 18 U.S.C. § 875(c), which prohibits sending a "communication containing any threat" to kidnap or injure a person in interstate commerce.[7] Despite the vile nature of the communications and the apparent applicability of the statute, the Sixth Circuit affirmed the trial court's dismissal of the indictment.[8] According to the court, for a communication to rise to the level of "threat," it must be "conveyed to effect some change or achieve some goal through intimidation."[9] Because Baker and Gonda neither sought change nor desired a particular goal, their terrifying rhetoric went unpunished.[10]

Cyberstalkers also use the Internet to facilitate their in-person stalking, often bypassing steps in the "course of conduct" required by many traditional stalking statutes,[11] as in the case of Amy Lynn Boyer.[12] She was stalked and later murdered while leaving work by Liam Youens, a man she did not know.[13] This tragedy is notable because Youens did not obtain Boyer's work address as stalkers normally do.[14] Instead, he purchased the information, as well as her

[4] *Id.*

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

[6] *Id.* at 1493 (majority opinion).

[7] *Id.*; 18 U.S.C. § 875(c) (2012).

[8] *Alkhabaz*, 104 F.3d at 1496.

[9] *Id.*

[10] *Id.*

[11] New Hampshire's stalking statute, for instance, prohibits a person from engaging in a "course of conduct targeted at a specific person which would cause a reasonable person to fear for his or her personal safety." N.H. REV. STAT. ANN. § 633:3-a (2013). The statute enumerates certain behavior included in a "course of conduct," like "[f]ollowing, approaching, or confronting . . . [or] [a]ppearing in close proximity to [the person]." *Id.* Notably absent are non-physical methods of information gathering.

[12] Chris Wright, *Murder.com: What Happened Last Fall on This Tiny New Hampshire Street Triggered a National Debate on Internet Crime. But was the Web Really to Blame for the Death of Amy Boyer?*, THE BOS. PHOENIX, Aug. 10, 2000, *available at* http://www.bostonphoenix.com/archive/features/00/08/10/MURDER.html.

[13] *Id.* After murdering Boyer, Youens turned his gun on himself. *Id.*

[14] *Id.*

social security number, from an online data broker called Docusearch.[15] As Youens himself acknowledged, "[i]t's actually obscene what you can find out about a person on the internet."[16]

Even newer technologies have provided individuals different means with which to harass.[17] Offensive communications on social networking websites like Facebook and Twitter present traditional First Amendment issues in unique contexts. In a recent example, William Cassidy allegedly posted hundreds of threatening Twitter messages, almost all aimed at American Buddhist figure Alyce Zeoli.[18] Cassidy argued that a conviction would impinge upon his First Amendment rights, and the District Court of Maryland agreed.[19] In defense of its position, the court analogized Twitter to colonial-era bulletin boards, leaving itself vulnerable to the criticism that its understanding of the medium lacks nuance.[20] Clearly, the courts are still grappling with the proper characterization of these websites and the nature of their communications, a difficulty that underscores the challenges inherent in creating viable statutory mechanisms for punishing cyberstalking.

"Cyberstalking by proxy"[21] further complicates the picture, as the recent Craigslist rape case demonstrates.[22] Jebidiah James Stipe created a false Craigslist posting in his ex-girlfriend's name in which he claimed that she had a rape fantasy.[23] Another man, Ty Oliver MacDowell, believing the ad to be legitimate, went to her house and raped her at gunpoint.[24] Stipe was indeed punished, but not under any cyberstalking laws.[25] Although this type of conduct seems like

---

[15] *Id.*

[16] *Id.*

[17] *See, e.g.*, Caroline Black, *Ex-Marine Jebidiah James Stipe Gets 60 Years for Craigslist Rape Plot*, CBS NEWS (June 29, 2010), http://www.cbsnews.com/8301-504083_162-20009162-504083.html; Somini Sengupta, *Case of 8,000 Menacing Posts Tests Limits of Twitter Speech*, N.Y. TIMES, Aug. 26, 2011, *available at* http://www.nytimes.com/2011/08/27/technology/man-accused-of-stalking-via-twitter-claims-free-speech.html; Bob Sullivan, *Vengeful Online Sex Ads Take Growing Toll*, THE REDTAPE CHRONICLES (July 27, 2010), http://redtape.msnbc.msn.com/_news/2010/07/27/6345571-vengeful-online-sex-ads-take-growing-toll.

[18] Sengupta, *supra* note 17.

[19] United States v. Cassidy, 814 F. Supp. 2d 574 (D. Md. 2011); *see infra* text accompanying notes 189–202.

[20] *Cassidy*, 814 F. Supp. 2d at 576; *see infra* text accompanying notes 189–202.

[21] Sullivan, *supra* note 17.

[22] Black, *supra* note 17.

[23] *Id.*

[24] *Id.*

[25] Stipe pleaded guilty to sexual assault, aggravated kidnapping, and aggravated burglary, and will serve a sixty-year prison sentence. *Id.*

exactly the type of harm that cyberstalking statutes should address, the current cyberstalking statutory regime is inadequate because both state and federal laws require the perpetrator to contact the victim directly.[26] Some commentators have called for amendments to address this shortcoming.[27]

The foregoing illustrates the insufficiency of the criminal law as presently constituted to address cyberstalking. While state and federal statutes exist, they often fail to criminalize conduct whose harms are self-evident, as in the cases above. When the statutes do cover such conduct, they do so in divergent ways. The resultant web of statutory prohibitions creates an incoherent system that does more harm than good.

This Comment argues that a unified federal approach is needed to remedy the problem and successfully control cyberstalking. Part II addresses the current state-by-state approach, arguing that it is both deficient from a policy perspective and violative of the Dormant Commerce Clause. Part III turns to the three federal statutes currently applied to quell cyberstalking, highlighting their own unique problems. Part IV advocates one federal law, drafted broadly enough to encompass the increasingly broad array of cyberstalking activities. More specifically, Part IV proposes that the federal government's primary cyberstalking statute be amended to remove unnecessary procedural roadblocks, to expand the bases for prosecution, to standardize the government's approach to cyberstalking, and to provide federal recourse for the victims of cyberstalking. By adopting these proposals, the federal government will begin repairing the significant inadequacies of the present system.

II. A STATE-BY-STATE APPROACH TO CYBERSTALKING LEGISLATION IS INAPPROPRIATE

It is undeniable that when we use the Internet, we do so without an appreciation of what state we are in.[28] The Internet is an incorporeal space, devoid of artificial boundaries and topographical landmarks.[29] As the District Court for the Southern District of New

[26] *See* Naomi Harlin Goodno, *Cyberstalking, A New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 MO. L. REV. 125, 152 (2007); *see infra* text accompanying notes 45–56, 214–216, 230–236.

[27] Goodno, *supra* note 26; *see infra* text accompanying notes 230–236.

[28] *See* American Libraries Ass'n v. Pataki, 969 F. Supp. 160, 167 (S.D.N.Y. 1997).

[29] *See* ACLU v. Reno, 929 F. Supp. 824, 837 (E.D. Pa. 1996) (the Internet is a "single body of knowledge").

York noted in *American Libraries Ass'n v. Pataki*, "geography . . . is a virtually meaningless construct on the Internet."[30] Given this reality, laws addressing conduct on the Internet should reflect the notion that state boundaries have no meaning on the Internet and that individuals are likely unaware of the variations between states' laws, or even, perhaps, in what state their Internet conduct is taking place.[31]

Nevertheless, states have enacted and modified a broad array of statutes that address cyberstalking.[32] These statutes fall into three general categories: (1) cyberstalking-specific laws;[33] (2) general stalking laws that have been amended to cover cyberstalking;[34] and (3) non-stalking laws applied to like conduct.[35] What follows is a brief survey of current state approaches to cyberstalking, through which a few things should become clear. The first is that states often have clever and efficient ways of drafting their statutes. Their methods vary widely, however, and while certain elements of these statutes are commendable, the resulting inconsistency creates confusion and competing obligations for the Internet user. Within the unique framework of the Internet landscape, this result should be impermissible.[36] And as will be explained further below, these laws—for many of the same reasons—also violate the Dormant Commerce Clause.

---

[30] *Pataki*, 969 F. Supp. at 169.

[31] *See id.*

[32] *See, e.g.*, ALASKA STAT. ANN. §§ 11.41.260, 11.41.270 (West 2006); ARK. CODE ANN. § 5-41-108 (West 2011); FLA. STAT. ANN. § 784.048 (West 2011); COLO. REV. STAT. § 602 (2010); 720 ILL. COMP. STAT. § 5/12-7.5 (2011); UTAH CODE ANN. § 106.5 (2008); 13 VT. STAT. ANN. § 1027 (2011); WYO. STAT. ANN. § 6-2-506 (1977).

[33] *See, e.g.*, 720 ILL. COMP. STAT. § 5/12-7.5.

[34] *See, e.g.*, WYO. STAT. ANN. § 6-2-506.

[35] *See, e.g.*, 13 VT. STAT. ANN. § 1027.

[36] Indeed, courts and commentators alike have long recognized the desirability of uniformity between the states in a wide variety of contexts. *See generally* Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1118 (9th Cir. 2007) (noting the inconsistency between states' intellectual property laws, and concluding that allowing state laws to regulate Internet-based intellectual property would "be contrary to Congress's expressed goal of insulating the development of the Internet from the various state-law regimes[]"); Kenneth W. Swenson, *A Stitch in Time: The Continental Shelf, Environmental Ethics, and Federalism*, 60 S. CAL. L. REV. 851, 882 (1987) (noting the need for uniform legislation in the context of environmental regulation); Wendy Trahan, *The Future of Sales and Use Tax on Electronic Commerce: Promoting Uniformity After* Quill, 21 VA. TAX REV. 101, 117–18 (2001) ("Uniform sales and use tax legislation may reduce the burden on electronic commerce businesses that are subject to varying state and local government collection obligations.")..

A. State Law Inconsistencies

Illinois is one of a few states that has passed a cyberstalking-specific statute. Its expansive law makes a first cyberstalking conviction a Class 4 felony.[37] The law provides that someone "commits cyberstalking when he or she engages in a course of conduct using electronic communication directed at a specific person, and he or she knows or should know that would cause a reasonable person to" either "fear for his or her safety or the safety of a third person" or "suffer other emotional distress."[38] A person also commits cyberstalking "when he or she, knowingly and without lawful justification, on at least 2 separate occasions, harasses another person"—or solicits his or her harassment—through the use of electronic communication by transmitting a threat that places a "person in reasonable apprehension of immediate or future bodily harm."[39]

Although these two provisions are fairly standard, the legislature also included language unique to other cyberstalking laws. Specifically, the law also punishes one who "creates and maintains an Internet website or webpage" that harasses a person, communicates a threat, or solicits an act that would violate the provision.[40] This subsection is important because it seemingly applies to the conduct of William Lawrence Cassidy, who, as mentioned above, was accused of posting threatening Twitter messages about Buddhist leader Alyce Zeoli.[41] Furthermore, the provision appears to reach the conduct of defendants Baker and Gonda in *Alkhabaz*, whose indictments under a federal statute were dismissed, the court finding that their conduct, though "sadistic," did not amount to "communication containing a threat."[42]

Whether Illinois's statute would address either the online information gathering of Liam Youens[43] or the "cyberstalking by proxy" of Jebidiah James Stipe,[44] however, is an open question, devoid of guiding case law. The statute would most likely not apply to

---

[37] 720 ILL. COMP. STAT. § 5/12-7.5.

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] Sengupta, *supra* note 17.

[42] United States v. Alkhabaz, 104 F.3d 1492, 1497–98 (6th Cir. 1997). The federal statue under which the defendants were charged was 18 U.S.C. § 875(c) (2012).

[43] Wright, *supra* note 12.

[44] Black, *supra* note 17.

Youens because of the "directed at a specific person" requirement. Although Youens did undergo a "course of conduct" directed at Boyer, it would be difficult to argue that the statutorily imperative portion of that course of conduct that occurred online was directed at her. The statute's applicability to Stipe's conduct is a closer call. While no provision within the statute fits his conduct directly, a court could interpret each of the three to cover "cyberstalking by proxy."

Mississippi's cyberstalking law contains four provisions,[45] and differs from Illinois's in certain respects.[46] Under this statute, it is unlawful for a person to use in electronic communication "any words or language threatening to inflict bodily harm."[47] Second, it is unlawful to repeatedly contact another person electronically "for the purpose of threatening, terrifying or harassing" that person.[48] The conduct prohibited by this provision would likely not be punishable by Illinois's cyberstalking law, though the ultimate determination would depend on the content of the messages. Third, it is unlawful to make false statements "concerning death, injury, illness, disfigurement, indecent conduct, or criminal conduct" about a person or his family "with the intent to threaten, terrify or harass."[49] Finally, it is unlawful to "[k]nowingly permit an electronic communication device under the person's control to be used for any purpose prohibited by this section."[50]

Although, again, the courts have been silent on the statute's application, the statute's language suggests that it fails to address all but the most conventional cyberstalking behavior.[51] For instance, its provisions require the offender to contact the victim directly;[52] therefore, the statute will not attach to the online postings of Jake Baker and Arthur Gonda,[53] the online information gathering of Liam Youens,[54] the malicious Twitter postings of William Lawrence Cassidy,[55] or the "cyberstalking by proxy" of Jebidiah James Stipe.[56]

Interestingly, North Carolina's cyberstalking statute mirrors

---

[45] MISS. CODE ANN. § 97-45-15 (West 2003).

[46] *Compare id.*, *with* 720 ILL. COMP. STAT. § 5/12-7.5 (2011).

[47] MISS. CODE ANN. § 97-45-15.

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *See id.*

[52] *Id.*

[53] *See* United States v. Alkhabaz, 104 F.3d 1492, 1496 (6th Cir. 1997).

[54] Wright, *supra* note 12.

[55] Sengupta, *supra* note 17.

[56] Black, *supra* note 17.

Mississippi's statute nearly word for word.[57] In fact, the only differences that can be found with respect to the prohibited conduct rest in the mens rea requirements of the second and third provisions.[58] Where in Mississippi the conduct is unlawful if it is committed with the intent to threaten, terrify, or harass,[59] the same conduct is unlawful in North Carolina if it is committed with the intent to "*abuse*, *annoy*, threaten, terrify, harass, or *embarrass*."[60] Neither legislature explains the difference in mens rea, but North Carolina's mens rea requirements reflect those in its pre-existing telephone harassment statute,[61] suggesting that the matter is more one of statutory continuity than one of legislative precision.

A more significant discrepancy between the two states' statutes, however, resides in the their respective punishments. In Mississippi, cyberstalking is a felony offense punishable by up to five years for a repeat offense; in North Carolina, on the other hand, cyberstalking is merely a Class 2 misdemeanor, with a maximum prison sentence of sixty days.[62] As a result, individuals found guilty of exactly the same conduct face the prospect of very different punishments depending on the location of the offense. It is this very type of disparity that renders the state statutory system so problematic.

Another approach that states take is to amend traditional stalking statutes to encompass cyberstalking behavior.[63] Wyoming's astutely composed stalking statute punishes someone who, with the intent to harass,

> engages in a course of conduct reasonably likely to harass that person, including but not limited to any combination of the following: (i) [c]ommunicating, anonymously or otherwise, or causing a communication with another person by verbal [or] electronic . . . means in a manner that

---

[57] *Compare* N.C. GEN. STAT. ANN. § 14-196.3 (West 2000), *with* MISS. CODE. ANN. § 97-45-15.

[58] *Compare* N.C. GEN. STAT. ANN. § 14-196.3, *with* MISS. CODE. ANN. § 97-45-15.

[59] MISS. CODE ANN. § 97-45-15.

[60] N.C. GEN. STAT. ANN. § 14-196.3 (emphasis added).

[61] N.C. GEN. STAT. ANN. § 14-196 (West 2000).

[62] MISS. CODE ANN. § 97-45-15 provides that cyberstalking is a "felony punishable by imprisonment for not more than two (2) years." If the communication contains a "credible threat," however, or if the offense is a repeat offense, then it is "punishable by imprisonment for no more than five (5) years. MISS. CODE ANN. § 97-45-15. In North Carolina, on the other hand, a class 2 misdemeanor carries a maximum prison sentence—even if the individual has committed five prior offenses—of sixty days in prison. N.C. GEN. STAT. ANN. § 15A-1340.23 (West 1995).

[63] *See, e.g.*, ALASKA STAT. ANN. §§ 11.41.260, 11.41.270 (West 2006); WYO. STAT. ANN. § 6-2-506 (1977).

> harasses; (ii) [f]ollowing a person . . . ; (iii) [p]lacing a person under surveillance . . . ; (iv) [o]therwise engaging in a course of conduct that harasses another person.[64]

The Wyoming legislature recognized that, today, stalking takes place both online and off, and that an appropriate legislative response should allow the punishable course of conduct to remain similarly fluid.[65] In recognition of this principle, the statute punishes acts that take place either online or in person, severing the distinction between traditional stalking and cyberstalking. Because of this, Wyoming's statute is the only law in this brief survey that would likely punish Liam Youens's covert online surveillance.[66] Moreover, its scope is broad enough that it might attach to Cassidy's Twitter rants[67] and Stipe's "cyberstalking by proxy."[68] In Wyoming, stalking is a misdemeanor.[69]

A final group of state statutes attempt to address cyberstalking without utilizing either cyberstalking or traditional stalking language.[70] For example, Vermont's most closely applicable statute makes it a crime to, "with intent to terrify, intimidate, threaten, harass or annoy," make contact with another and

> (i) make[] any request, suggestion or proposal which is obscene, lewd, lascivious or indecent; (ii) threaten[] to inflict injury or physical harm to the person or property of any person; or (iii) disturb[], or attempt[] to disturb, by repeated anonymous telephone calls or other electronic communications, whether or not conversation ensues[.][71]

Despite the absence of specific stalking or cyberstalking terminology,[72] the statute's language reflects that of many other

---

[64] WYO. STAT. ANN. § 6-2-506(b) (1977).

[65] *Id.*

[66] Wright, *supra* note 12.

[67] Sengupta, *supra* note 17.

[68] Black, *supra* note 17.

[69] WYO. STAT. ANN. § 6-2-506 (1977).

[70] *See, e.g.*, VA. CODE ANN. § 18.2–60 (2002).

[71] 13 VT. STAT. ANN. § 1027.

[72] Vermont's law does, however, contain an interesting jurisdictional provision. "An offense committed . . . as set forth in this section shall be considered to have been committed at either the place where the telephone call or calls originated or at the place where the communication or communications or calls were received." *Id.* This language is strange, because, according to a plain reading of the provision, when the crime's setting is based on the "origination," rather than the "receipt," of a message, only a telephone call may form the basis of jurisdiction. If the message was created on a computer, the only place where a crime may be committed is where the message was received. Though no findings state so explicitly, this discrepancy may be an attempt to avoid the problem of states prosecuting out-of-state residents who

states, and would probably apply both to Cassidy's Twitter harassment[73] and to Stipe's "cyberstalking by proxy."[74] It would likely not, however, punish Jake Baker, Arthur Gonda,[75] or Liam Youens,[76] because it requires the individual to make contact with the victim.[77] Given the statute's similarity to those of other states, it is perhaps strange that a conviction under this statute exposes the defendant to a maximum punishment of only three months of imprisonment and a fine of $250.00[78]—a true disparity when viewed in light of other states' responses.[79]

This brief survey of state cyberstalking statutes demonstrates that states have different opinions about the harms that cyberstalking presents, and different approaches in addressing them. While these laws contain valuable provisions that the federal government would be wise to adopt, the significant overlap between them creates a web of inconsistency that, as a public policy matter, should render them unenforceable.[80] The Internet landscape is too devoid of cognizable boundaries to allow individual states to carve out wide prohibitions.

B. The State Approach Violates the Dormant Commerce Clause

Not only are the inconsistencies in the state-law approach problematic from a public policy perspective, these inconsistencies also render the state statutes violative of the Dormant Commerce Clause. As a general matter, the Dormant Commerce Clause "is the principle that state and local laws are unconstitutional if they place an undue burden on interstate commerce."[81] If a law does not

contact victims within the state. Then again, it is difficult to see why that rationale would not extend to telephone communications as well as computer communications.

[73] Sengupta, *supra* note 17.

[74] Black, *supra* note 17.

[75] *See* United States v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997).

[76] Wright, *supra* note 12.

[77] 13 VT. STAT. ANN. § 1027.

[78] *Id.*

[79] In Illinois, cyberstalking is a class 4 felony. 720 ILL. COMP. STAT. § 5/12-7.5 (2011). Under Illinois law, a class 4 felony is punishable by a sentence of "not less than one year and not more than three years." 730 ILL. COMP. STAT. 5/5-4.5-45 (2012). In Mississippi and North Carolina, as noted, the maximum sentences are five years and sixty days, respectively. *Supra* note 6262. In Rhode Island, the sentence can be as long as two years. R.I. GEN. LAWS ANN. § 11-52-4.2 (West 2008).

[80] For a similar view on the "smorgasbord" of state cyberstalking law, *see* Harry A. Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2, 70–77 (2004).

[81] ERWIN CHEMERINSKY, CONSTITUTIONAL LAW, PRINCIPLES AND POLICIES 419 (Vicki Been et al. eds., 3d ed. 2006).

discriminate against non-residents, then the court employs a balancing test first articulated in *Pike v. Brace Church, Inc.*[82] According to this test, a facially nondiscriminatory law that regulates a legitimate local interest and has only incidental effects on interstate commerce "will be upheld unless the burden imposed upon such commerce is clearly excessive in relation to the putative local benefits."[83]

As commentators have noted, however, the Dormant Commerce Clause "does not end with the *Pike* Test."[84] State laws may also be struck down on the bases of "extraterritoriality" or "inconsistent obligations."[85] The "extraterritoriality" doctrine was central to the Supreme Court's decision in *Healy v. Beer Inst., Inc.*[86] At issue in *Healy* was a Connecticut statute that required out-of-state beer shippers to affirm that their prices were no higher than prices in the surrounding states.[87] The Court surveyed its extraterritoriality decisions, finding that the Dormant Commerce Clause invalidated state laws that regulated commerce taking place wholly outside of the state.[88] In such a case, it did not matter whether the statute's "extraterritorial reach was intended by the legislature."[89] More important were the practical effects of the regulation and the statute's potential interaction with other states' legitimate statutory regimes.[90] Because the affirmation statute had "the undeniable effect of controlling commercial activity occurring wholly outside the boundary of the State," the Court invalidated it.[91]

State laws may also violate the Dormant Commerce Clause in another—and not entirely unrelated—way.[92] If a law has the potential to "subject an area of interstate commerce to inconsistent state regulation," the Dormant Commerce Clause is violated.[93] This

---

[82] 397 U.S. 137 (1970).

[83] *Id.* at 142.

[84] *See, e.g.*, Chi Pann, Comment, *The Dormant Commerce Clause and State Regulation of the Internet: Are Laws Protecting Minors From Sexual Predators Different From Those Protecting Minors From Sexually Explicit Materials?*, 2005 DUKE L. & TECH. REV., No. 8, at 5 (2005).

[85] *Id.* at 5–6.

[86] 491 U.S. 324 (1989).

[87] *Id.*

[88] *Id.* at 336 (citing Edgar v. MITE Corp., 457 U.S. 624, 642–43 (1982)).

[89] *Id.*

[90] *Id.* at 336–37.

[91] *Id.* at 337.

[92] *See* Cooley v. Bd. of Wardens of Port of Phila., 53 U.S. 299 (1851).

[93] Pann, *supra* note 84, at 17 (citing Bibb v. Navajo Freight Lines, Inc., 359 U.S. 520, 529–30 (1959) (striking down a state highway regulation); S. Pac. Co. v. Sullivan, 325 U.S. 761, 779–82 (1945) (striking down a state railroad regulation)).

principle has its roots in early Commerce Clause analysis.[94] In *Cooley*, the Court noted that "[w]hatever subjects of this power are in their nature national, or admit only of one uniform system, or plan of regulation, may justly be said to be of such a nature as to require exclusive legislation by Congress."[95] The Court thus recognized that some conduct, by its very nature, requires a uniform set of laws, only appropriately provided by Congress.[96]

Of the three tests, the *Pike* test is the most clearly defined, and is generally accepted amongst commentators.[97] Beyond that, however, disputes arise. Some persuasively argue that the extraterritoriality and inconsistent obligations bases are merely considerations under the *Pike* test.[98] Meanwhile, others maintain that those tests are distinct from the *Pike* test, and are independently sufficient to invalidate state laws.[99] A third contingent reads the jurisprudence as endorsing two of the above three tests.[100] Despite the confusion, these tests clearly inform modern Dormant Commerce Clause analysis, and all three have been used to evaluate state laws that regulate Internet use, most notably in *American Libraries Ass'n v. Pataki*.[101] Because the statute at issue in *Pataki* resembles the cyberstalking statutes at issue here,[102] the *Pataki* decision serves as an important touchstone for the Dormant Commerce Clause analysis of state cyberstalking laws.

---

[94] *See Cooley*, 53 U.S. at 299.

[95] *Id.* at 319.

[96] *Id.*

[97] Pann, *supra* note 84, at 18.

[98] For instance, Goldsmith and Sykes present a compelling argument that the "real concern underlying the extraterritoriality and inconsistent-regulations prongs of dormant Commerce Clause analysis is not out-of-state effects and nonuniformity per se, but rather whether the out-of-state burdens of a regulation outweigh its local benefits." Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785, 827 (2001).

[99] Pann, *supra* note 84, at 18.

[100] Michael W. Loudenslager, although acknowledging the three doctrines do at least nominally exist in the jurisprudence, notes that courts have treated the "inconsistent obligations" test "as effectively a preemption analysis." Michael W. Loudenslager, *Allowing Another Policeman on the Information Superhighway: State Interests and Federalism on the Internet in the Face of the Dormant Commerce Clause*, 17 BYU J. PUB. L. 191, 230 (2003). Loudenslager recognizes the *Pike* balancing test and, relying heavily on *Healy*, the extraterritoriality analysis as the two bases for invalidating nondiscriminatory state laws under the Dormant Commerce Clause. *Id.* at 213–17. Peter C. Felmy goes in a different direction, suggesting that the "extraterritoriality" rationale be separated from Dormant Commerce Clause analysis altogether. Peter C. Felmy, *Beyond the Reach of the States: The Dormant Commerce Clause, Extraterritorial State Legislation, and the Concerns of Federalism*, 55 ME. L. REV. 467 (2003).

[101] 969 F. Supp. 160 (S.D.N.Y. 1997).

[102] *See supra* Part II.A.

Pataki pitted a broad array of interest groups and organizations against the Governor and the Attorney General of New York.[103] At issue was the constitutionality of a New York law that made it a felony to knowingly transmit to a minor, using a computer, material that is harmful to minors.[104] The court concluded that the statute violated the Dormant Commerce Clause on all three of the grounds detailed above—the *Pike* balancing test, extraterritoriality, and inconsistent obligations.[105]

First, the court addressed the extraterritoriality defect of the New York law.[106] The court noted that the "nature of the Internet makes it impossible to restrict the effects of the New York Act to conduct occurring within New York."[107] Non-New Yorkers, in other words, could not prevent their transmissions from entering New York. This made them potentially subject to the New York statute's jurisdiction.[108] As a result, the statute had the practical effect of regulating conduct wholly outside of the state.[109] This encroachment, the court held, rendered the New York Act "per se violative of the [Dormant] Commerce Clause."[110]

Next, the court analyzed the law under the *Pike* balancing test.[111] While the court accepted that protecting children against pedophilia was a legitimate state interest, it held that any benefit derived from the law was outweighed by its burden on interstate commerce.[112] For one, the statute would not—indeed could not—have an effect on international communications.[113] Further, the effective prosecution of the statute would require pursuing out-of-staters, and that process would be "beset with practical difficulties."[114] And because New York

---

[103] These organizations included: American Library Association, Freedom to Read Foundation, Inc., New York Library Association, Westchester Library System, American Booksellers Foundation For Free Expression, Association of American Publishers, Bibliobytes, Magazine Publishers of America, Interactive Digital Software Association, Public Access Networks Corporation, ECHO, New York City Net, Art on the Net, Peacefire, and the American Civil Liberties Union. *Pataki*, 969 F. Supp. at 161–62.

[104] *Id.* at 161–63. The law at issue was N.Y. Penal Law § 235.21.

[105] *Id.* at 169; *see* Pann, *supra* note 84.

[106] *Pataki*, 969 F. Supp. at 173.

[107] *Id.* at 177.

[108] Pann, *supra* note 84, at 21.

[109] *Pataki*, 969 F. Supp. at 177.

[110] *Id.*

[111] *Id.*

[112] *Id.* at 177–78.

[113] *Id.* at 178.

[114] *Id.*

had other laws aimed at preventing similar harms, any benefits would be confined to the narrow class of cases falling outside the scope of existing laws.[115] The court balanced this relatively minor benefit against the law's significant burdens on interstate commerce, including the "extreme burden" on interstate commerce, the "chilling effect" on out of state Internet users, and the "excessive" costs of enforcement.[116] Because, on balance, the burdens of the law on interstate commerce outweighed its local benefits, the law failed the *Pike* test and violated the Dormant Commerce Clause. [117]

Finally, the court decided that the statute was invalid because it risked imposing upon individuals inconsistent obligations.[118] The court, channeling *Cooley*, noted,

> [t]he courts have long recognized that certain types of commerce demand consistent treatment and are therefore susceptible to regulation only on a national level. The Internet represents one of those areas; effective regulation will require national, and more likely global, cooperation. Regulation by any single state can only result in chaos, because at least some states will likely enact laws subjecting Internet users to conflicting obligations.[119]

As an illustration of the difficulties that would attend the upholding of the law, the court referred to the legal standard upon which conviction would turn.[120] The material sent must be "harmful to minors," which was defined, in part, as being "patently offensive to prevailing standards in the adult community as a whole."[121] The problem with this standard is that "there is no single 'prevailing community standard' in the United States."[122] Therefore, to avoid the possibility of prosecution, the Internet user must either comply with the most stringent regulation or forego communication entirely.[123] Because the risk of imposing inconsistent obligations is impermissible under the Dormant Commerce Clause, the court struck down the law.[124]

In the wake of *Pataki*, other courts struck down similar laws,

---

115 *Pataki*, 969 F. Supp. at 179.

116 Pann, *supra* note 844, at 23 (citing *Pataki*, 969 F. Supp. at 179–80).

117 *Pataki*, 969 F. Supp. at 181.

118 *Id.*

119 *Id.*

120 *Id.* at 182.

121 *Id.*

122 *Id.*

123 *Pataki*, 969 F. Supp. at 183.

124 *Id.*

largely employing the same rationale as the *Pataki* court.[125] Not all courts, however, were persuaded. The courts in the latter category—overwhelmingly (and perhaps unsurprisingly) state courts—drew distinctions between the statute at issue in *Pataki* and those at issue in their cases, concluding that their statutes satisfied the Dormant Commerce Clause.[126]

Representative of those cases is a California decision, *Hatch v. Superior Court*.[127] *Hatch* involved a statute similar to that in *Pataki*, making it "a criminal offense to send, *by any means*, specified harmful matter to a minor 'with the intent or for the purpose of seducing a minor.'"[128] Despite the similarities to the statute in *Pataki*, the California law survived its Dormant Commerce Clause challenge.[129] The court distinguished *Pataki* on two grounds. First, the court focused on the "intent-to-seduce" requirement. In the court's view,

> a ban on communication of specified matter to a minor *for purposes of seduction* can only affect the rights of the very narrow class of adults who intend to engage in sex with minors. We have found no case which gives such intentions or the communications employed in realizing them protection under the dormant Commerce Clause.[130]

In other words, because the commerce in question was not legal under the laws of California, the Dormant Commerce Clause should not apply.[131]

Second, the court held that the statute would not likely affect interstate commerce, citing California penal statutes that prevent punishment for wholly extraterritorial offenses.[132] The court thus upheld the statute.[133]

Hatch and similar cases,[134] however, were wrongly decided. The distinctions the *Hatch* court drew from the statute in *Pataki* are, under

---

[125] *See* PSINet, Inc. v. Chapman, 362 F.3d 227 (4th Cir. 2004); Am. Booksellers Found. v. Dean, 342 F.3d 96 (2d Cir. 2003); ACLU v. Johnson, 194 F.3d 1149 (10th Cir. 1999); Cyberspace Commc'ns, Inc. v. Engler, 142 F. Supp. 2d 827 (E.D. Mich. 2001).

[126] *See* People v. Hsu, 99 Cal. Rptr. 2d 184 (Cal. Ct. App. 2000); Hatch v. Sup. Ct., 94 Cal. Rptr. 2d 453 (Cal. Ct. App. 2000); State v. Heckel, 24 P.3d 404 (Wash. 2001).

[127] 94 Cal. Rptr. 2d 453.

[128] *Id.* at 459 (citing CAL. PENAL CODE § 288.2(a) (West 2012)).

[129] *Id.*

[130] *Id.* at 472.

[131] *See id.*

[132] *Id.* at 473.

[133] *Hatch*, 94 Cal. Rptr. 2d at 473. The *Hsu* court utilized this same argument as well. People v. Hsu, 99 Cal. Rptr. 2d 184, 191–92 (Cal. Ct. App. 2000).

[134] *See, e.g.*, *Hsu*, 99 Cal. Rptr. 2d 184; State v. Heckel, 24 P.3d 404 (Wash. 2001).

scrutiny, untenable. The *Hatch* court's first error was the weight that it afforded the statute's mens rea requirement. The reason that the intent element was important, it declared, was because it narrowed the range of banned conduct—it would, in the court's words, "only affect the rights of the very narrow class of adults who intend to engage in sex with minors."[135] Echoing that sentiment, California's Fifth District Court of Appeal noted, in a similar case, *People v. Hsu,* that "it is difficult to conceive of any *legitimate commerce* that would be burdened by penalizing the transmission of harmful sexual material known to minors in order to seduce them."[136] These courts erred in their failure to recognize that the legitimacy or illegitimacy—that is, the legality or illegality—of commerce is itself a legal conclusion, dependent upon the particular law that a court is referencing.

For example, consider the statute at issue in *Hatch* and *Hsu*, which prohibited sending harmful material to a minor "with the intent or for the purpose of seducing a minor."[137] Because states have different ages of consent, an adult in one state could be seducing someone online whom he legitimately believes to be of age in his state. In his own state, he would not be committing a crime, because the object of his seduction, by his own state's law, would not be a minor. But because his target happens to reside in California—a fact he may have no way of knowing—he would be subject to prosecution in California. Because, in these cases the legitimacy of commerce depends upon standards particular to state law, the commerce's legitimacy or illegitimacy will vary from state to state. Therefore, the courts' reliance on mens rea was an ineffective distinction from the result in *Pataki*.

The *Hatch* court's second error was its reliance on California's general bar on "punishment for wholly extraterritorial offenses"[138] as an indication that California would not pursue out-of-state offenders for these types of crimes. As Alex McDonald notes, California courts have repeatedly upheld convictions of individuals for crimes whose results occurred in California, but whose conduct took place wholly outside of California.[139] An even more recent example confirms this

---

[135] *Hatch*, 94 Cal. Rptr. 2d at 471.

[136] *Hsu*, 99 Cal. Rptr. 2d at 190 (emphasis added). *Hsu* involved the same statute that was at issue in *Hatch*. *Compare id.* at 192, *with Hatch*, 94 Cal. Rptr. 2d at 463.

[137] CAL. PENAL CODE § 288.2(a) (West 2012).

[138] *Hatch*, 94 Cal. Rptr. 2d at 473.

[139] Alex C. McDonald, *Dissemination of Harmful Matter to Minors Over the Internet*, 12 SETON HALL CONST. L.J. 163 (2001). As McDonald notes:

> In Ex Parte Hedley [31 Cal. 108 (1866)], the California Supreme Court upheld the embezzlement conviction in California under California

point. In *People v. Betts*, the Supreme Court of California held that "a state may exercise jurisdiction over criminal acts that take place outside of the state if the results of the crime are intended to, and do, cause harm within the state."[140] So even though it might be true that California will not pursue out-of-state offenders for wholly extraterritorial crimes, it is equally true that the conduct at issue in *Hatch* and *Hsu* was not wholly extraterritorial, because its results took place within the state.[141]

Moreover, even if it may be true that "there is no reason to suppose California would attempt to impose its policies on other states,"[142] statutes that regulate extraterritorially are "invalid regardless of whether the statute's extraterritorial reach was intended by the legislature."[143] Furthermore, the statute must be considered in light of "what effect would arise if not one, but many or every, State adopted similar legislation."[144] While it might be true that California would not pursue out-of-state offenders, as a logical matter, if at least one state permits prosecution of out-of-state conduct, then the entire Internet community is subject to inconsistent obligations. The user will have to abide by the laws of his state as well as the laws of the state that extends its reach beyond its geographical boundaries. Therefore, under *Healy*, even if California truly did not intend to assert its extraterritorial reach, the statute would still be invalid.[145]

As a result of the weaknesses in the *Hatch* line of cases, *Pataki*

> law of the defendant, who in Nevada drew checks on his employer's account and sent them to California to be cashed. In People v. Sansom [37 Cal. App. 435 (C.A. Sec. Dis. Cal. 1918)], the California court upheld the forgery (uttering) conviction in California under California law of the defendant, who forged a check in Mexico and sent it to his agent in California for deposit in an Arizona bank. Receipt in California of an Internet communication sent from another state seems indistinguishable from receipt in California of a forged check sent from another state. It therefore appears that California criminal jurisdiction permits prosecution in California under section 288.2(b) California Penal Code of a person who sends an Internet communication from another state that is received in California, and otherwise satisfies the elements of the statute.

Id. at 213–14.

[140] People v. Betts, 23 Cal. Rptr. 3d 138, 142 (Cal. 2005).

[141] *See Hatch*, 94 Cal. Rptr. 2d 453; *Hsu*, 99 Cal. Rptr. 2d 184.

[142] *Hatch*, 94 Cal. Rptr. 2d at 473.

[143] Healy v. Beer Inst., Inc., 491 U.S. 324, 336 (1989). The *Hsu* court betrays its ignorance of this critical point by noting that the statute "makes no reference to place of performance, so courts must assume the Legislature did not intend to regulate conduct taking place outside the state." *Hsu*, 99 Cal. Rptr. 2d at 192.

[144] *Healy*, 491 U.S. at 336.

[145] *Id.* at 336.

emerges as the more persuasive authority both from a legal and public policy perspective. The principles that drove the decision in *Pataki* are highly relevant to the legitimacy of the state statutory approach to cyberstalking. Consider, for example, a hypothetical Dormant Commerce Clause analysis of the Illinois cyberstalking statute, applying the principles at work in *Pataki*.[146]

C. A Dormant Commerce Clause Analysis of Illinois's Cyberstalking Statute

First, we must consider the extraterritoriality doctrine. Under *Healy*, a statute "that directly controls commerce occurring wholly outside the boundaries of a State" is invalid under the Dormant Commerce Clause.[147] If the practical effect of the law is to control conduct in other states, it is invalid, regardless of the legislature's intent.[148] Illinois's law contains no geographic limitation; its provisions apply to all electronic communication, without reference to where the sender physically resides.[149] Under a plain reading of the law, an individual outside of Illinois could initiate online contact with an individual in Illinois and violate any of the three provisions of the law, subjecting himself to prosecution in Illinois. Perhaps the Illinois law's final provision draws this into clearest relief:[150] a person who creates a webpage about another person does not directly communicate with his victim; rather, he displays his message to the Internet community at large, in whatever state the recipient may reside. Because the website's creator does not have control over where his website is accessible, he must either comply with Illinois's unique law or forgo his communication entirely. This is precisely the choice to which the extraterritoriality doctrine is directed, and as a result the Illinois statute violates the Dormant Commerce Clause.

If the *Pataki* court's application of the *Pike* test is accepted, it will also doom Illinois's statute. As mentioned, the *Pike* test involves a two-step inquiry.[151] First, the court must examine the legitimacy of the state's interest. It is difficult to contest the validity of the interest here, and a court would most likely assume its validity. Next, the court must determine whether the burden to interstate commerce

---

146 Recall Illinois's cyberstalking-specific statute. *Supra* Part II.A.

147 *Healy*, 491 U.S. at 336.

148 *Id.*

149 720 ILL. COMP. STAT. § 5/12-7.5 (2011).

150 *See supra* text accompanying notes 37–40.

151 Pike v. Brace Church, Inc., 397 U.S. 137, 142 (1970).

outweighs the state's interest.[152] It was at this point that the *Pataki* court balked, and the court's arguments resonate in this context as well. First, the "practical difficulties" involved with enforcement of the statute reduce the significance of the local benefit—for example, Illinois could not prevent online harassment from international sources.[153] It also might be cost prohibitive to prosecute individuals whose only contact with the state "occurs via the Internet."[154] Furthermore, the "chilling effect" discussed in *Pataki* is also present here, and "Internet users will steer clear of the Act by significant margin," thereby burdening interstate commerce.[155] For these reasons, the Illinois law would probably be invalidated under the *Pike* test as well.

Finally, the Illinois statute violates the Dormant Commerce Clause on the basis of the inconsistent obligations it imposes on Internet users. Every state espouses different values, and these values are inevitably reflected in the state's legal code. Illinois's statute—and in particular subsection (a)(5)—is unique.[156] It is not an unreasonable provision, but at this point, Illinois is the only state to employ such language.[157] In every other state—assuming the language in other states' statutes will not be stretched beyond cognizance—such conduct is legal. But an Internet user creating or maintaining such an Internet site in any other state must be aware not only of the laws of his own state, but also of this Illinois law. These are precisely the inconsistent obligations that violate the Dormant Commerce Clause.[158]

This Comment does not argue that the state statutes are, by and large, poorly drafted, or that they are wrongheaded responses to the social ills wrought by cyberstalking. Instead, this Comment argues that a state-by-state approach to cyberstalking reflects poor public policy and violates the Dormant Commerce Clause. These laws reach beyond their states' boundaries, they impose inconsistent obligations upon Internet users, and by and large they impose a greater burden on interstate commerce than is justified by the harm they target. In

---

[152] *Id.*

[153] *See* Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 171 (S.D.N.Y. 1997).

[154] *Id.* at 178.

[155] *Id.* at 179.

[156] 720 ILL. COMP. STAT. § 5/12-7.5 (2011).

[157] *See id.*

[158] Here we again witness the overlap between the extraterritoriality and inconsistent obligations doctrines. While this overlap exposes the uncertainty of current law, it does not undermine the legal conclusions derived from the doctrines.

the "decentralized, global communications medium"[159] that is the Internet, these scattered laws are an incomplete and unsatisfying solution. Because cyberstalking and the harms that it creates routinely "travel" across state boundaries, sound jurisprudence and public policy demonstrate that an appropriate response to cyberstalking is a unified federal system. The ideal federal approach will utilize the best parts of the state statutes—like Illinois's creation-or-maintenance-of-a-website provision and Wyoming's implicit recognition that much stalking activity today vacillates fluidly between online and offline conduct—and simultaneously remedy the state-by-state approach's significant shortcomings.

III. THE CURRENT FEDERAL APPROACH TO CYBERSTALKING IS LACKING

Today, three federal statutes apply to adult cyberstalking behavior.[160] One provision of one statute[161] is directed specifically at cyberstalking; the others are slightly different statutes that courts have adapted to cyberstalking as a matter of convenience.[162] As a practical matter, however, the cyberstalking statute and other applicable statutes constitute an inefficient and substandard regime. The following section describes the existing statutes and addresses their respective deficiencies.

A. 18 U.S.C. § 2261A

This statute is the federal government's primary vehicle for combating stalking and cyberstalking. It contains two provisions, one dedicated to each. Section (1) is a fairly broad physical stalking statute.[163] It serves its limited purpose well, but standing alone it is an

---

[159] *Pataki*, 969 F. Supp. at 164.

[160] *See* 18 U.S.C. § 2261A (2006); 18 U.S.C. § 875 (2006); 47 U.S.C. § 223 (2006). Another statute, 18 U.S.C. § 2425, prohibits the transmission of certain information to a minor with the "intent to entice, encourage, offer, or solicit any person to engage in any sexual activity for which any person can be charged with a criminal offense." 18 U.S.C. § 2425 (2006). While this statute certainly has value, it is aimed at a different harm than the harm discussed in this Comment, and is outside of its scope. For a discussion of the application of cyberstalking law to children, *see* Kimberly Wingteung Seto, *How Should Legislation Deal With Children as the Victims and Perpetrators of Cyberstalking?*, 9 CARDOZO WOMEN'S L.J. 67 (2002).

[161] 18 U.S.C. § 2261A.

[162] 18 U.S.C. § 875; 47 U.S.C. § 223; 18 U.S.C. § 2425.

[163] 18 U.S.C. § 2261A(1).

> Whoever . . . travels in interstate or foreign commerce . . . with the intent to kill, injure, harass, or place under surveillance with intent to kill, injure, harass, or intimidate another person, and in the course of, or as a result of, such travel places that person in reasonable fear of the death of, or serious bodily injury to, or causes substantial emotional

insufficient tool to combat cyberstalking.

Section (2) is the federal government's cyberstalking provision.[164] Given its importance, it is reproduced below, in full.

> Whoever
>
> (2) with the intent—
>
> (A) to kill, injure, harass, or place under surveillance with intent to kill, injure, harass, or intimidate, or cause substantial emotional distress to a person in another State or tribal jurisdiction or within the special maritime and territorial jurisdiction of the United States; or
>
> (B) to place a person in another State or tribal jurisdiction, or within the special maritime and territorial jurisdiction of the United States, in reasonable fear of the death of, or serious bodily injury to—
>
> (i) that person;
>
> (ii) a member of the immediate family (as defined in section 115) of that person; or
>
> (iii) a spouse or intimate partner of that person;
>
> uses the mail, any interactive computer service, or any facility of interstate or foreign commerce to engage in a course of conduct that causes substantial emotional distress to that person or places that person in reasonable fear of the death of, or serious bodily injury to, any of the persons described in clauses (i) through (iii) of subparagraph (B); shall be punished as provided in section 2261(b) of this title.[165]

For reasons explained below, this provision has been used sparingly. But when the government has employed the statute, it has proved effective. In *United States v. Bowker*, the victim, Tina Knight, began receiving threatening and vulgar e-mails from several different e-mail addresses.[166] An initial FBI investigation of the communications revealed Erik Bowker as the sender, and Knight

---

> distress to that person, a member of the immediate family (as defined in section 115) of that person, or the spouse or intimate partner of that person.

Id.

[164] 18 U.S.C. § 2261A(2).

[165] *Id.*

[166] 372 F.3d 365, 371 (6th Cir. 2004), *vacated*, 543 U.S. 1182 (2005).

procured a cease and desist order.[167] Bowker, however, continued to send threatening e-mails, phone calls, and letters both to Knight and to her family, suggesting that he would use violence against her.[168] Furthermore, Bowker traveled from his residence in Ohio to Knight's in West Virginia to take photographs of her place of work and to steal her mail.[169] On appeal, the Sixth Circuit found that Bowker "intended to instill in Knight a fear of death or serious bodily harm through use of the mails and other facilities of interstate commerce," and that he was guilty under § 2261A(2).[170]

In *United States v. Rose*, a California man, Richard Rose, was accused of cyberstalking a Minnesota woman, Lois Fischer.[171] The two had met online while playing a card game, and a romance blossomed.[172] They exchanged "cyber vows" and agreed to meet in California, while Fischer was on a business trip.[173] When the time came, however, Fischer got cold feet, and she refused to meet Rose.[174] Rose tracked her down to her hotel and called her on the telephone.[175] But when Fischer's husband answered (Fischer had told him she was widowed), Rose became enraged, and responded by sending her a barrage of vulgar and threatening e-mails, including death threats to Fischer's children.[176] Rose also posted pictures of Fischer's children online, "along with their full names, address, and telephone number, on web sites soliciting sexual activity."[177] Perhaps unsurprisingly, Rose was convicted under § 2261A(2).[178]

One recent case is also worthy of note. Shawn Memarian pleaded guilty to cyberstalking under § 2261A(1) in early 2009.[179] Memarian had dated his victim—a Missouri, then Colorado, resident—for approximately one month.[180] After the relationship

---

[167] *Id.* at 372.

[168] *Id.*

[169] *Id.* at 373.

[170] *Id.* at 388. Bowker was appealing his convictions under 18 U.S.C. § 2261A(1), 47 U.S.C. § 223(a)(1)(C), and 18 U.S.C. § 1708. *Id.* at 370, 388.

[171] 315 F.3d 956, 957 (8th Cir. 2003).

[172] *Id.*

[173] *Id.*

[174] *Id.*

[175] *Id.*

[176] *Id.*

[177] *Rose*, 315 F.3d at 957.

[178] *Id.* at 956. Rose was also convicted under 18 U.S.C. § 875(c). *Id.*

[179] United States v. Memarian, 371 Fed. Appx. 711, 711 (8th Cir. 2010).

[180] News Release, U.S. Dep't of Justice, KC Man Sentenced for Cyberstalking: False Website Ads Invited Strangers to Victim's Home for Sexual Encounters (June 17, 2009), *available at* http://www.justice.gov/usao/mow/news2009/memarian.sen

ended, Memarian began a wide-ranging course of online harassment.[181] He sent her "more than 75 threatening e-mails."[182] Worse, Memarian, posing as his victim, created false personal ads describing the victim as a "sex freak," which he posted on MySpace and Facebook.[183] In all, approximately thirty men responded to the ads, some showing up to the victim's house at night.[184] What is notable about Memarian's plea is that it might suggest that his latter conduct—"cyberstalking by proxy"[185]—falls within the reach of § 2261A(2). But given that there was no trial—and that Memarian's sending of seventy-five threatening e-mails alone would likely have been sufficient to garner a conviction under § 2261A(2)—concluding so may be premature.

Indeed, some commentators are convinced that § 2261A(2) would not cover "cyberstalking by proxy," like that of Jebidiah James Stipe.[186] According to Naomi Harlin Goodno, for all the good § 2261A(2) does, it still fails to "squarely deal with situations where the cyberstalker pretends to be the victim and encourages third parties to innocently harass the victim, such as posting sexual invitations on a message board in the name of the victim to dupe third parties to respond."[187] Given the increasing prevalence of such conduct, an effective federal statute should clearly encompass this harm.

An even more recent case, mentioned previously, adds an interesting twist to the general applicability and efficacy of § 2261A. William Lawrence Cassidy was charged with cyberstalking under section § 2261A(2)(A) for a series of Twitter and blog postings directed at Buddhist figure Alyce Zeoli.[188] Under a series of aliases, Cassidy unleashed a virulent barrage of messages directed at Zeoli.[189] These messages ranged from pointed religious criticism ("(A.Z.) is a demonic force who tries to destroy Buddhism") to sinister and thinly veiled threats ("Rain tomorrow should cover the tracks").[190] In the end, Cassidy published about 8,000 tweets, most directed towards

.htm.

[181] *Id.*

[182] *Id.*

[183] *Id.*

[184] *Id.*

[185] Sullivan, *supra* note 17.

[186] Black, *supra* note 17.

[187] Goodno, *supra* note 26, at 152.

[188] United States v. Cassidy, 814 F. Supp. 2d 574, 576 (D. Md. 2011).

[189] *Id.*

[190] *Id.* app. A.

Zeoli.[191]

In December 2011, the District Court for the District of Maryland dismissed Cassidy's indictment, holding that, as applied to Cassidy, § 2261A(2)(A) was an unconstitutional infringement on his First Amendment right to free speech.[192] In reaching its conclusion, the court relied on a few important propositions. First, the court analogized Twitter to a colonial-era bulletin board.[193] Like a bulletin board, which can be ignored simply by not walking over to the board, Twitter allows users to ignore messages they do not want to view by either "blocking" or "unfollowing" the sender of the offending messages.[194] According to the court, "[t]his is in sharp contrast to a telephone call, letter or e-mail specifically addressed to and directed at another person, and that difference . . . is fundamental to the First Amendment analysis in this case."[195] Specifically, this distinction meant the difference between the presence and absence of an important government interest.[196] The Fourth Circuit has held, for instance, that in the context of a telephone harassment statute, the government does have a "strong and legitimate" interest.[197] But because a Twitter user may disregard the offensive messages, that same government interest is not present.

The second critical aspect of the case was that Zeoli is a prominent religious figure. Amici pointed out that Zeoli's own Twitter account has 17,221 followers, and she has produced instructional videos that have been viewed over 143,000 times.[198] Because she is an "easily identifiable public figure that leads a religious sect," the statute implicated types of expression that the Supreme Court has consistently attempted to protect.[199]

While at first blush the decision in this case casts doubts upon the continuing validity of § 2261A(2)(A), *Cassidy* will not be the last word on this cyberstalking statute. For one, this as-applied holding is readily distinguishable, as most stalking cases do not involve

---

[191] Sengupta, *supra* note 17.

[192] *Cassidy*, 814 F. Supp. 2d at 583.

[193] *Id.* at 576.

[194] *Id.* at 577.

[195] *Id.* at 578.

[196] *Id.*

[197] *Id.* at 585 (citing Thorne v. Bailey, 846 F.2d 241, 243 (4th Cir. 1988)).

[198] *Cassidy*, 814 F. Supp. 2d. at 586 n.14. Indeed, one can watch her official enthronement as Jetsunma Akhon Lhamo, the reincarnation of an important Buddhist figure. ENTHRONEMENT OF JETSUNMA AKHON LHAMO, http://www.tara.org/jetsunma-ahkon-lhamo/biography/ (last visited Jan. 2, 2012).

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

prominent religious figures. Secondly, and possibly more critically, the court's bulletin board analogy fails to withstand scrutiny. Although the court's description of Twitter was accurate, the court glossed over the fact that Zeoli could not actually easily ignore Cassidy's messages. She did attempt to ignore his tweets, but each time she blocked him, Cassidy created a new alias with which to harass Zeoli.[200] In all, Cassidy employed thirteen different usernames.[201] Thus, while Cassidy's speech was not quite as direct as a telephone call or e-mail, it is difficult to limit Twitter messages to the "public forum" designation, especially given the particular facts of the case. Given the importance of the bulletin board analogy to the court's disposition, it is puzzling that it chose to ignore this seemingly critical fact.

A final shortcoming of § 2261A(2) is its overly cautious reach. The statute's applicability is significantly narrowed by the requirement that the offender and the victim be in different states. This restriction appears designed to protect against a potential Commerce Clause challenge, but it is an unnecessary restriction because the use of the Internet alone is enough to satisfy the Commerce Clause.[202] By including this limitation, Congress effectively constrained prosecution to a small subset of potential cases. The limitation, for instance, would preclude prosecution in a case like Jebidiah James Stipe's, if Stipe had been in the same state as his victim. That Stipe's cyberstalking conduct could go unpunished merely by virtue of an invisible and meaningless state line approaches the absurd. Furthermore, in light of the deficiencies in the state approach, it becomes clearer still that a proper federal statute must have the maximum possible breadth.

---

[200] Kashmir Hill, *You Have a Constitutional Right to Stalk and Harass People on Twitter*, FORBES, Dec. 16, 2011, *available at* http://www.forbes.com/sites/kashmirhill/2011/12/16/you-have-a-constitutional-right-to-stalk-and-harass-people-on-twitter/.

[201] *Cassidy*, 814 F. Supp. 2d at 579 n.7.

[202] *See* U.S. v. MacEwan, 445 F.3d 237 (3d Cir. 2006) (holding that the Internet is an instrumentality of interstate commerce, and Congress has the Commerce Clause power to regulate the transmission of child pornography even if transmission did not cross state lines). Furthermore, courts' treatments of the next statute, 18 U.S.C. § 875, underscore the point. Section 875 contains no such limiting language, and courts have held that threatening Internet communications can be prosecuted even where the defendant and the recipient reside in the same state. *See* United States v. Kammersell, 196 F.3d 1137 (10th Cir. 1999); United States v. Morales, 272 F.3d 284 (5th Cir. 2001).

B. 18 U.S.C. § 875

This statute, entitled "Interstate Communications," contains a provision that in certain cases applies to cyberstalking.[203] Subsection (c) prohibits communication containing a threat.[204] This provision is infrequently applied, and has garnered only a few convictions of note.[205] The limitation is that the statute requires a "threat." The usual interpretation of a "true," or "credible threat," was expressed in *United States v. Kelner*,[206] where the court held that a threat must be an "unequivocal, unconditional and specific expression[] of intention immediately to inflict injury."[207] This high threshold excludes a broad array of cyberstalking activity that does not convey such a narrowly construed menace.[208]

Unfortunately, at least one court has adopted an even more restrictive standard.[209] In *United States v. Alkhabaz*—the case that affirmed the dismissal of Jake Baker and Arthur Gonda's indictments under § 875—the Sixth Circuit announced that to amount to a "threat," the communication "must be such that a reasonable person (1) would take the statement as a serious expression of an intention to inflict bodily harm (the mens rea), and (2) would perceive such expression as being communicated to effect some change or achieve some goal through intimidation (the actus reus)."[210] The dissent in *Alkhabaz* took strong issue with the majority's extrajudicial addition of an element into the statute.[211] The judge noted that even though

[203] 18 U.S.C. § 875 (2012).

[204] 18 U.S.C. § 875(c).

[205] One such conviction came in an aforementioned case, United States v. Rose, 315 F.3d 956, 957 (8th Cir. 2003); *see also* United States v. Sutcliffe, 505 F.3d 944 (9th Cir. 2007) (transmitting interstate threats to injure and transferring social security numbers of various targets on website); United States v. Newell, 309 F.3d 396 (6th Cir. 2002) (sending "harassing and threatening" e-mails to ex-girlfriend); United States v. Scott, 42 F. App'x. 264 (10th Cir. 2002) (sending threatening e-mails); *Morales*, 272 F.3d 284 (entering Internet chat room and threatening to shoot and kill students at school); United States v. Johnson, 18 F. App'x 463 (9th Cir. 2000) (sending e-mail threats to kill judicial officer); *Kammersell*, 196 F.3d 1137 (sending a bomb threat by instant message).

[206] 534 F.2d 1020 (2d Cir. 1976).

[207] *Id.* at 1027.

[208] For an argument that the "credible threat" standard is outdated, *see* Joanna Lee Mishler, *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, 121–29 (2000).

[209] *See* United States v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997).

[210] *Id.* at 1495.

[211] *Id.* at 1506 (Krupansky, J., dissenting).

certain communications under § 875 would satisfy the constitutional "threat" standard, they would nonetheless be immune from prosecution because, as here, they "were not made with the intent to realize a specific purpose through intimidation."[212]

A related problem with § 875 is that its language does not appear to allow a "course of conduct" to amount to a threat: the menace must be transmitted through one message.[213] Given that much of the fear generated from cyberstalking is derived from continual contact, rather than a single isolated threat, this statute's applicability is limited. Although § 875 may be useful in certain egregious situations, it is not valuable in cyberstalking cases where the fear is supplied by the stalker's continual contact with the victim, rather than by the content of the messages themselves.

C. 47 U.S.C. § 223

In 2006, Congress amended this longstanding telephone harassment statute[214]—enacted in 1934—"to ensure that e-mail messages sent via the Internet were covered by § 223."[215] Today, "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" is guilty of sending "obscene or harassing" communications.[216] While this statute has proven useful in the past,[217] several issues render it ineffective.

First, it may be unconstitutional. The "intent-to-annoy" requirement has posed problems in similar statutes.[218] In *Coates v. City of Cincinnati*, for example, the Supreme Court struck down an ordinance that forbid residents to assemble in groups and comport themselves in an "annoying" manner.[219] The Court found that the statute was unconstitutionally vague because conduct that "annoys some people does not annoy others."[220] Therefore, "no standard of

---

[212] *Id.*

[213] 18 U.S.C. § 875(c) (2006).

[214] 47 U.S.C. § 223 (2006).

[215] Goodno, *supra* note 26, at 148.

[216] 47 U.S.C. § 223(a)(1)(C) (2006).

[217] It was, for example, used to garner a conviction in United States v. Bowker, 372 F.3d 365 (6th Cir. 2004), *see infra* text accompanying notes 225–229.

[218] *See* Coates v. City of Cincinnati, 402 U.S. 611 (1971); Bolles v. People, 189 Colo. 394 (1975).

[219] 402 U.S. at 611.

[220] *Id.* at 614.

conduct is specified at all."[221] Similarly, in *Bolles v. People*, the court struck down a harassment statute that required the intent to "harass, annoy, or alarm"[222] on the ground that it was facially overbroad.[223] According to the court, forbidding annoying and alarming communications would render illegal discussing "anything that is of any significance . . . . The First Amendment is made of sterner stuff."[224]

Only one court has ruled on the constitutionality of the mens rea in § 223.[225] In the aforementioned case of *United States v. Bowker*, the Sixth Circuit upheld the law.[226] In justifying its defense of the statute, the court read together the mens rea requirements to give them similar meanings.[227] So while "annoy" alone may be unconstitutionally vague, the court held that when it is associated with words like "threaten" and "harass," its meaning can be easily understood.[228] The statutes at issue in *Coates* and *Bolles*, however, were not substantially different than the statute at issue in *Bowker*.[229] Given this, and considering that the *Bowker* court is the only court thus far to address the issue in the context of § 223, it would be rash to conclude that § 223 passes constitutional muster.

But even granting the provision constitutional satisfaction does not repair its other, and arguably more substantial, infirmities. Goodno isolates two important problems.[230] First, the fact that the statute requires the communicator to be anonymous is problematic.[231] This element, "without reason," prevents prosecution in cases where the victim knows the stalker.[232] This problem seems especially weighty given that "[m]ore than fifty-nine percent of female stalking victims (and thirty percent of male stalking victims) are stalked by an intimate partner[.]"[233] Second, "the statute applies only to direct

---

[221] *Id.*

[222] 189 Colo. at 395 n.1.

[223] *Id.* at 399.

[224] *Id.* at 398.

[225] United States v. Bowker, 372 F.3d 365 (6th Cir. 2004).

[226] *Id.*

[227] *Id.* at 382–83.

[228] *Id.*

[229] *Compare* 47 U.S.C. § 223 (2006) ("intent to annoy, abuse, threaten, or harass any person"), *with* the statutes at issue in Coates v. City of Cincinnati, 402 U.S. 611, 612 (1971) ("conduct . . . annoying to persons passing by") *and Bolles*, 189 Colo. at 395 n.1 ("intent to harass, annoy, or alarm another person").

[230] Goodno, *supra* note 26, at 150.

[231] *Id.*

[232] *Id.*

[233] Laura Silverstein, *The Double Edged Sword: An Examination of the Global*

communications between the stalker and victim, e.g., the statute would only be triggered when the cyberstalker sends an e-mail directly to the victim."[234] Therefore, the statute would apply neither to Jebidiah James Stipe's "proxy cyberstalking,"[235] nor to William Lawrence Cassidy's indirect Twitter harassment.[236] These types of conduct are increasingly relevant, and that this statute fails to punish them is a major shortcoming.

In sum, all three federal statutes that are applied to cyberstalking have deficiencies that render them ineffectual, both individually and in combination. While the jurisdictional expansiveness of § 875 is better than its sharply delimited counterpart in § 2261A(2), § 875's heightened "threat" threshold precludes its application in swaths of important cases. And while § 223's sprawling mens rea requirements—that certainly skirt, if not breach, constitutional limits—expand the potential convictions, its other limitations lessen its effectiveness, without really broadening the federal government's reach. What is needed, therefore, is comprehensive federal legislation that will incorporate the best parts of existing federal and state statutes.

IV. PROPOSAL

Congress has recognized the need for reform in cyberstalking legislation.[237] Their proposed revisions—specifically with respect to § 2261A—do not, however, go far enough.[238] Cyberstalking reform must also include amendments that broaden the scope of punishable acts, remove jurisdictional impediments, and, in order to ensure effective enforcement, provide victims a private cause of action.

First, Congress should amend § 2261A(1) by removing the requirement that the stalker cross state lines, and require only that a portion of the cyberstalker's course of conduct take place online. Recall that Wyoming's stalking statute reflected the increasingly

Positioning System, Enhanced 911, and the Internet and Their Relationships to the Lives of Domestic Violence Victims and Their Abusers, 13 BUFF. WOMEN'S L. J. 97, 120 (2006).

[234] Goodno, *supra* note 26, at 150.

[235] Black, *supra* note 17.

[236] Sengupta, *supra* note 17.

[237] *See* Stalkers Act of 2011, S. 224, 112th Cong. (2011), *available at* http://thomas.loc.gov/cgi-bin/query/z?c112:S.224.IS:.

[238] Amended § 2261A(b)(1) would remove the requirement that the stalker and victim be in different states where the stalker "uses the mail, any interactive computer service, or any other facility of interstate or foreign commerce." *Id.* By suggesting this change, Congress appears to have recognized what this Comment earlier suggested: that the use of the Internet itself satisfies the Commerce Clause.

common reality that stalkers use the Internet as a tool to facilitate traditional, in-person stalking.[239] In that sense, cyberstalking can be a means, rather than an end.[240] Liam Youens did not use the Internet as a means of torment, but as a way to collect information about Amy Lynn Boyer so that he could be a more effective stalker in the physical world.[241] When stalkers use the Internet as a virtual alternative to monitoring movements in person, the online pursuit should be no less culpable than the physical pursuit. The law must recognize that when stalkers use the Internet, they utilize a facility of interstate commerce, and, as a result, the requirement that they physically cross state lines becomes superfluous. It limits the number of cases that the federal government can pursue, without adding value. When a portion of the stalker's course of conduct takes place online, the law must not also require that the stalker physically cross state lines.

The amended statute must also explicitly recognize that the "following" of a victim—language that appears in Wyoming's law[242]—may occur online, and must be included within the prohibited "course of conduct." The current version of § 2261A(2) prohibits the use of "the mail, any interactive computer service, or any facility of interstate or foreign commerce to engage in a *course of conduct* that causes substantial emotional distress to that person[.]"[243] By its terms, online information gathering about a victim would not be punishable. It is difficult, for instance, to assert that a victim will have suffered emotional distress from being pursued online when the victim is unaware he or she is being pursued. When the online course of conduct extends beyond covert intelligence gathering into malicious harassment, then § 2261A(2) clearly kicks in. But when the only online activity goes unnoticed by the victim, § 2261A(2) appears not to apply.

Returning to the Boyer case underscores this point.[244] Boyer

[239] Wyoming's statute defined the punishable course of conduct to include any of the following: "(i) [c]ommunicating, anonymously or otherwise, or causing a communication with another person by verbal, electronic . . . means in a manner that harasses; (ii) [f]ollowing a person . . . ; (iii) [p]lacing a person under surveillance . . . ; (iv) [o]therwise engaging in a course of conduct that harasses another person." WYO. STAT. ANN. § 6-2-506 (1977).

[240] *See* Wright, *supra* note 12.

[241] *Id.* Recall Youens's own opinion on the matter: "It's accually [sic] obsene [sic] what you can find out about a person on the internet." *Id.*

[242] WYO. STAT. ANN. § 6-2-506 (1977).

[243] 18 U.S.C. § 2261A(2) (2012) (emphasis added).

[244] We will ignore, for now, that Youens eventually murdered Boyer. *See* Wright, *supra* note 12.

never noticed Youens's Internet activity.[245] By its own terms, § 2261A(2) most likely does not apply, because Youens's online course of conduct did not cause his victim substantial emotional distress.[246] But § 2261A(1) would not apply either, because Youens did not cross state lines in his physical pursuit of Boyer. Amending § 2261A(1) to allow prosecution when the stalker utilizes the Internet, but does not cross state lines, as well as explicitly recognizing that mere online information gathering is a part of the culpable course of conduct, repairs this infirmity.

Next, Congress should amend § 2261A(2) by removing the requirement that the stalker and victim be in different states. As previously noted, *United States v. MacEwan* held that the Internet is a channel and an instrumentality of interstate commerce; therefore, the Commerce Clause regulates the transmission of child pornography over the Internet even if the transmission does not cross state lines.[247] In so holding, the court analogized the Internet to other traditional instrumentalities of interstate commerce, such as bridges, railways, and airplanes.[248] Moreover, *MacEwan* was not an isolated holding. In *United States v. Extreme Assocs.*, the court held that the "Internet is a channel of commerce covered by the federal statutes regulating the distribution of obscenity."[249]

Therefore, the requirement in § 2261A(2) that the victim be "a person in another State" is unnecessary when the Internet is involved. Despite Congress's initial reticence, it seems to have recognized this important point of law more recently. Its proposed amendment to § 2261A states that "[i]t shall be unlawful for any person, with intent to kill, physically injure, harass, or intimidate another person, to engage in a course of conduct . . . that uses the mail, any interactive computer service, or any other facility of interstate or foreign commerce[.]"[250] This amendment is important for two related reasons. First, it would remove the current requirement that the victim and stalker be in different states.[251] Second, the language used—"that uses the mail, any interactive computer service, or any *other* facility of interstate or foreign commerce"[252]—suggests that

---

[245] *Id.*

[246] 18 U.S.C. § 2261A(2)(B).

[247] 445 F.3d 237 (3d Cir. 2006).

[248] *Id.* at 245 n.8.

[249] 431 F.3d 150, 161 (3d Cir. 2005).

[250] Stalkers Act of 2011, S. 224, 112th Cong. (2011), *available at* http://thomas.loc.gov/cgi-bin/query/z?c112:S.224.IS:.

[251] 18 U.S.C. § 2261A(2)(B).

[252] Stalkers Act of 2011, S. 224, 112th Cong. (2011) (emphasis added), *available at*

Congress considers an interactive computer service a facility of interstate commerce. Congress should speedily adopt this revision.

Next, Congress should insert a provision similar to one present in Illinois's law.[253] As noted above, the law makes it a crime to "create[] and maintain[] an Internet website or webpage which is accessible to one or more third parties" that either "communicates a threat . . . [or] places that person or a family member of that person in reasonable apprehension of immediate or future bodily harm . . . or solicits the commission of an act" that would be a violation of Illinois's code.[254] This type of language appears to cover two types of conduct: "cyberstalking by proxy," and conduct like that of William Lawrence Cassidy, where there is no direct communication between the stalker and victim.[255]

This Comment's final suggestion returns again to the Boyer case. After her murder, Boyer's estate brought suit against Docusearch for providing Youens with the information that led to her killing.[256] Docusearch argued that it owed no duty to Boyer, and the District Court for the District of New Hampshire certified the question to the New Hampshire Supreme Court.[257] The Supreme Court imposed a duty on Docusearch.[258] In so concluding, the court began with the general rule that "[a]ll persons have a duty to exercise reasonable care not to subject others to an unreasonable risk of harm."[259] Duty does not arise solely from relationships, the court noted, but also "from the need for protection against reasonably foreseeable harm."[260] Generally, however, because "actor[s] may reasonably proceed upon the assumption that others will obey the law," criminal misconduct is unforeseeable.[261] There are three exceptions to this general rule: (1) where a special relationship exists; (2) where special circumstances exist; and (3) where the duty has been voluntarily assumed.[262] There are special circumstances "where there is 'an especial temptation and opportunity for criminal misconduct

http://thomas.loc.gov/cgi-bin/query/z?c112:S.224.IS:.

[253] 720 ILL. COMP. STAT. § 5/12-7.5 (2011).

[254] *Id.*

[255] Sengupta, *supra* note 17.

[256] Remsburg v. Docusearch, No. CIV. 00-211-B, 2002 WL 844403, at *1 (D.N.H. Apr. 25, 2002).

[257] *Id.*

[258] Remsburg v. Docusearch, 816 A.2d 1001, 1006 (N.H. 2003).

[259] *Id.*

[260] *Id.* (citing Hungerford v. Jones, 722 A.2d 478, 480 (N.H. 1998)).

[261] *Id.* (citing Walls v. Oxford Mgmt. Co., 633 A.2d 103, 105 (N.H. 1993)).

[262] *Id.* at 1007.

brought about by the defendant.'"[263] After all, where one creates a situation that "involves an unreasonable risk of harm to another," he or she has a duty to prevent that risk from occurring.[264] regardless of whether the "exact occurrence or precise injuries" were foreseeable.[265] Critically, the court held that the rise in cyberstalking has created just such a foreseeable risk.[266] Therefore, the court held, if a data broker like Docusearch's "disclosure of information to a client creates a foreseeable risk of criminal misconduct against the third person whose information was disclosed, the investigator owes a duty to exercise reasonable care not to subject the third person to an unreasonable risk of harm."[267]

Congress should follow in the footsteps of the New Hampshire Supreme Court and include in § 2261A a private cause of action for victims of cyberstalking against data brokers who have breached a duty of reasonable care to the people whose information they sell.[268] Incorporating such a remedy would facilitate the government's goals. After all, the provision's very existence would create a disincentive to data brokers to haphazardly provide private individuals' sensitive information to others. By cutting off the dissemination of this private information at its source, the government should be able to prevent—rather than punish—cyberstalking.

V. CONCLUSION

When the worlds of crime and technology collide, law enforcement is always left fighting to keep up. Advances arrive at a head-spinning rate, and criminals tend to be quick learners. Despite the government's best intentions, it has not been able to keep pace with technological "advancements" in cyberstalking. New ways to distribute and collect information have supplanted older and established means, allowing cyberstalkers to skirt the edges of established law. By necessity, the states and Congress have attacked the problem in piecemeal fashion, addressing specific problems when they arise. While these stopgap measures were no doubt justified when they were first contemplated, the resulting collection of

[263] *Id.* (citing *Walls*, 663 A.3d at 106).

[264] *Remsburg*, 816 A.2d at 1007.

[265] *Id.* (citing Iannelli v. Burger King Corp., 761 A.2d 417, 420 (2000)).

[266] *Id.* at 1008.

[267] *Id.* at 1007.

[268] For a discussion on the applicability of the tort of intrusion in this context, *see* William Dalsen, Comment, *Civil Remedies for Invasions of Privacy: A Perspective on Software Vendors and Intrusion upon Seclusion*, 2009 WIS. L. REV. 1059 (2009).

divergent approaches created a muddled system of overlapping obligations. Simplifying the federal government's approach while broadening its reach will eliminate confusion and allow the federal government to pursue a wide range of dangerous criminals. Adopting these proposed revisions and excising the state approach should correct some of the current ills, and protect some currently vulnerable victims.