Cyberstalking and the Internet Landscape We Have Constructed

MERRITT BAER†

There is no world like the one surfacing.

-Joy Harjo, Emergence

ABSTRACT

Criminalizing behavior online will necessarily test constitutional rights in novel ways; cyberstalking, as a crime of accumulated words, overtly challenges the First Amendment. This article shows the disconnect between the rationale for criminalizing cyberstalking and the application and enforcement of statutes addressing stalking online. The multidimensional harms in cyberstalking force us to transcend a kinetic-world framework and recognize that the Internet is not merely a new medium for speech but rather a space in which actions occur. Because patterns of victimization create dynamics of domination, cyberstalking’s impact inserts itself into and molds the Internet landscape. This article argues for a consistent set of legal tools selected for their correlation to our ethical borders and our sense of where the damage from cyberstalking lies. To accomplish this end, Internet citizens will need to choose a coherent set of values to live by online.

† Merritt Baer is originally from Colorado and a graduate of Harvard College and Harvard Law School. She has work experience in high-tech, law firm and government sectors, with a special interest in Internet law, cybercrime and cyber war.
TABLE OF CONTENTS

I. Framing the Problem of Cyberstalking ................................................................. 154
   A. A New Forum for an Old Problem, or a Distinct Problem? .......................... 155
   B. Factors that Facilitate Stalking Online ......................................................... 156
   C. Cyberstalking Laws ......................................................................................... 158
   D. Problems with Cyberstalking Statutes ............................................................. 160
      1. How kinetic must the harm be? ................................................................. 160
      2. Problems with both “credible threats” doctrine and the “reasonable person” standard ................................................................. 160
II. Cyberstalking Statutes and the First Amendment ......................................... 162
   A. Accepted Rationales for First Amendment Abridgements .............................. 162
      1. Criminal Threats, Hate Speech and “Fighting Words” .................................. 162
      2. Low-Value Speech ....................................................................................... 164
      3. General Overview of the Court’s Trajectory ................................................. 164
      4. Internet as a Forum ...................................................................................... 166
III. Not All Are Cyberstalked Equally ................................................................. 166
   A. Patterns of Online Abuse ................................................................................. 167
      1. Unlike cancer, cyberstalking is a social disease .......................................... 167
      2. Our stake in our online persona creates new vulnerabilities (for cyberstalkers to exploit) ................................................................. 169
      3. Who is harmed by patterns of cyberstalking? ................................................ 169
IV. Conclusion: Where do we go from here? ....................................................... 170

I. Framing the Problem of Cyberstalking

Stalking is a unique crime in that it is composed of a series of otherwise legal acts. Cyberstalking in particular is composed of words alone and therefore stands more distinctly as apart as a crime of accumulation. As one sociologist described it, "the separated acts that make up the intrusion cannot by themselves cause the mental abuse, but do taken together (cumulative effect)." The cumulative nature of the crime makes it hard to pinpoint or to prosecute. In this article, I show that existing laws do not effectively address cyberstalking. I add, in addition, I argue that as Internet citizens, we have a stake in correcting cyberstalking’s toxic impact on the cyber landscape.

Cyberstalking is important both in its own right and as a case study on the types of harms emerging online and the ways these online harms confound current legal instruments. Cyberstalking harms individuals in ways that are hard to criminalize and eludes law enforcement tools because of its complicated constitutional implications. Its victims fall along demographic and social lines, highlighting both online gender inequality and the line between the tech-savvy and the tech-naïve. Cyberstalking matters not only because it is a source of terror for certain individuals, but because its harm shapes the Internet

---

landscape that we all inhabit. Because of cyberstalking, the Internet, heralded as an opportunity for equalization in interaction, seems in many ways to have become a world of domination after all.

A. A New Forum for an Old Problem, or a Distinct Problem?

Early cyberstalking literature views cyberstalking as an extension of the act of stalking into a new forum; however, even up-to-date sources claim, “While the differences between the two forms of stalking must be acknowledged, it is most important to acknowledge that cyberstalking is fundamentally an extension of the physical act.”2 I disagree with this characterization because First Amendment concerns separate cyberstalking from physical stalking, and cyberstalking gives rise to different forms of harm than physical stalking. I therefore contend that lawmakers and enforcers ought to use different factors for identifying and prosecuting cyberstalking.

The story of Rebecca Schaeffer first thrust stalking into the American consciousness when her stalker murdered her on July 18, 1989.3 California enacted the first stalking law soon after, on Jan. 1, 1991. In addition to criminalizing stalking, it prohibited the Department of Motor Vehicles from divulging addresses upon request.4 Cyberstalking has gained more recognition recently, as it is now recognized as a crime. The societal acknowledgement of cyberstalking seems to track two major factors. First, it corresponds to the growing willingness to acknowledge kinetic–world stalking as a problem.5 Second, it may be attributable to some of the lethal cyberbullying cases, like that of Megan Meier.6

Attempts to correlate cyberstalking to the kinetic-world do have downfalls. The law’s focus on kinetic-world damage is one problematic starting point in the current approach to cyberstalking. Even now, most disciplines, including law, persist in trying to draw connections between cyberstalking and kinetic-world damage—but was the harm to Megan Meier lesser the moment or hour or day before her suicide than it was after her death? The definition of cyberstalking seems disconnected from the instances in which

---

2 Wayne Petherick, Cyber-Stalking: Obsessional Pursuit and the Digital Criminal, http://www.trutv.com/library/crime/criminal_mind/psychology/cyberstalking/5.html, (last visited Apr. 28, 2010). Petherick cites Casey: “The overarching message here is that we should concentrate on the details, the uniqueness and complexity of a case rather than get caught up on typologies, terminology or the fact that we are dealing with a different medium.” Interview with E. Casey (Feb. 3, 1999). I posit, however, that the cyber medium is elemental to the crime, not a detail of it. See also PAUL E. MULLEN ET AL., STALKERS AND THEIR VICTIMS 183-185 (2d ed. 2009) (identifying cyberstalking as a new location, and not a different manifestation, of stalking).


4 Obtaining addresses in this manner was previously routine practice. Schaeffer’s killer, Robert John Bardo, paid $1 to find her residence, where he killed her. See CAL. PENAL CODE §646.9 (Deering 2010), which has evolved through the years. Section 646.91a prohibits stalkers from obtaining a victim’s address or location. See also CAL. VEH. CODE §1808.21 (Deering 2009) (enacted in the wake of Schaeffer’s murder, requiring confidentiality in DMV records generally).

5 I use kinetic to refer to the physical, non-cyber world.

stalking is taken seriously. For example, even the statute California enacted in 1991 would not have addressed Schaeffer’s stalker. Until 1994, the statute required that a stalker make a “credible threat of death or great bodily injury”\(^7\) to the victim, and that the victim feel a reasonable sense of fear as a result.\(^8\) Neither Schaeffer nor Theresa Saldana, whose stalker stabbed her in the torso ten times in 1982, were aware of their respective stalker-murderers’ threats; even if they had known, the threats themselves were implied and not direct.\(^9\)

### B. Factors that Facilitate Stalking Online

Several aspects of the online experience explain the recent proliferation of cyberstalking incidents and reports.\(^10\) First, the lack of inhibition inherent in online communications may embolden people to speak violently online who would not act so boldly offline. Thus, individuals “who may not otherwise engage in offline stalking” may nevertheless engage in cyberstalking.\(^11\) Likewise, the divulgence of many details of one's life may lead a potential stalker to feel a false sense of intimacy with his victim.\(^12\)

\(\text{\textsuperscript{7}}\) §442.


\(\text{\textsuperscript{9}}\) Unlike Saldana, whose first contact with her stalker was his attack, Schaeffer’s stalker-murderer sent threats but her producers never informed her of them. See LINDEN GROSS, SURVIVING A STALKER: EVERYTHING YOU NEED TO KNOW TO KEEP YOURSELF SAFE 190 (2000); Christina Perez, Stalking: When Does Obsession Become a Crime?, 20 AM. J. CRIM. L. 263, 268–69 (1993).

\(\text{\textsuperscript{10}}\) Aggregated cyberstalking numbers are not available—in part, of course, because they often could also fall under the rubric of crimes like identity theft and other forms of online abuse. See Alexis A. Moore, Cyberstalking and Women: Facts and Statistics (2009), http://womensissues.about.com/od/violenceagainstwomen/a/CyberstalkingFS.htm. As far back as 1996-97, a study published in the Attorney General’s report on cyberstalking found that of the 13% of female students who were stalked, 24.7% of those women were also being contacted by their stalker by email; by 2009, a study at a “mid-Atlantic university” found that 13% of all students were victims of cyberstalking. See, respectively, U.S. DEP’T OF JUSTICE, 1999 REPORT ON CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY (1999), http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm; and Karen L. Paullet, Daniel R. Rota and Thomas T. Swan, Cyberstalking: An Exploratory Study of Students at a Mid-Atlantic University, Vol. X No. 2 ISSUES IN INFORMATION SYSTEMS 640 (2009) available at http://www.iciis.org/iis/2009_iis/pdf/P2009_1212.pdf. Paullet et al. write, “This study argues that cyberstalking and harassment will only decrease when the extent of the problem is fully understood and potential victims and law enforcement understand the protections necessary under the law.”

\(\text{\textsuperscript{11}}\) PAUL BOCU, CYBERSTALKING: HARASSMENT IN THE INTERNET AGE AND HOW TO PROTECT YOUR FAMILY 90–106 (Prager 2004). Some comments by the head of a British cyberstalking study acknowledge this online effect of “giving courage to cowards”:

Tom Ilube, CEO of web security experts Garlik, which carried out the research, said he was surprised at the number of people cyberstalked, adding it could even be more aggressive than being stalked in person.

He said: “I think it’s the same sort of harassment that people will do offline, but it becomes easier to do from behind a computer screen. It takes some sort of twisted courage to ring someone and harass them, but there’s definitely a feeling of power sitting behind a PC screen. People will do things they would never do in person or over the phone.


same vein, a false sense of intimacy online may make the "stalker" feel more comfortable than s/he should when deciding what information to post.  

Second, online mechanisms can even facilitate stalking. Whereas a stalker used to have to pick up the phone, stamp a letter or drive to the victim’s house, now s/he can send an “email bomb” triggering thousands of spam emails to the victim, or post something disparaging that arrives on hundreds of online message boards by morning. "[T]he Internet is a borderless medium that allows instantaneous and anonymous distribution of one’s message," and the stalker has the protection of the “veil of anonymity.” Yet tangibly, in some ways the cyber-forum is more intimate than anything else—with increased computer and Internet use in the workplace, access in airports and airplanes, and the web-enabled handheld device, abuse can be enacted anywhere and can enter every facet of the victim’s life. For example, wireless tracking is easy for the tech-savvy cyberstalker—s/he can tandem on cell phones and trace a person's physical whereabouts, or (especially if the cyberstalker had a former relationship with the victim), install a keylogger. This could be an almost infinite source of intimate and potentially destructive information.

Third, the existence of a subversive Internet counterculture may encourage cyberstalking. As reported by Mattathias Schwartz in his exploration into the dark world of popular Internet counterculture site 4chan and their message board /b/, “Measured in terms of depravity, insularity and traffic-driven turnover, the culture of /b/ has little precedent.” This particular brand of computer–enacted violence is encapsulated in the concept of “Lulz,” which is the trolls’ measure of success. ‘Lulz’ means the joy of disrupting another's emotional equilibrium. ‘Lulz’ is watching someone lose their mind at their computer 2,000 miles away while you chat with friends and laugh.’³⁸

¹³ A 2007 study led by Paige Padgett from the University of Texas Health Science Center found that women looking for love online assumed there was a false degree of safety. See Paige Padgett, Personal Safety and Sexual Safety for Women Using Online Personal Ads, 4 SEXUALITY RES. AND SOC. POL’Y: J. OF NSRC, June 2007, at 27, 27 (“The high frequency and intensity of e-mail communication prior to meeting in person cultivated acceleration of intimacy for the individuals involved and may have affected women's decisions to engage in risky sexual behaviors.”).


¹⁶ http://en.wikipedia.org/wiki/Keylogger. A quick Google search of keylogging reveals a number of companies selling affordable keylogging tools. Obviously, someone who has physical or password access to their stalking victim will have an even easier time installing a keylogger—and gains full knowledge of the content of the victim’s typing, including passwords.


¹⁸ Id. (“Prominent ‘troll’ Fortuny created a harassing blog after Meiers’ death called ‘Megan Had It Coming.’ Fortuny explicitly stated that the blog was intended ‘to question the public’s hunger for remorse and to challenge the enforceability of cyberharassment laws like the one passed by Megan’s town after her
Finally, the likelihood of reporting may be higher for crimes where the victim generally knows a crime is being committed (as opposed to, say, child pornography). Theoretically there may also exist higher potential for reporting of cyberstalking versus kinetic-world stalking because cyberstalking is composed of written words and it is thus easier to keep records. Conversely, without physical acts to use as evidence, victims may also hesitate longer before reporting cyberstalking to law enforcement.

C. Cyberstalking Laws

At the state level, all fifty states and the District of Columbia have enacted stalking and harassment laws; forty-six states explicitly include electronic forms of communication within these laws. The laws vary in terms of conduct criminalized, standards that may trigger prosecution, penalties for violations, and protections afforded victims. At least six states have adopted separate statutes specifically targeting cyberstalking.

Federally, four major laws, in addition to one directed at minors, apply to cyberstalking:

1) The Interstate Communications Act

This prohibits transmitting a threat to injure someone in interstate commerce via any communication (e.g., by telephone, email, or beeper). However, 18 U.S.C § 875(c) is often inapplicable to cyberstalking because it requires an overt threat.

2) The Telephone Harassment Act, as amended by the 2000 Violence Against Women Act (VAWA)

The Telephone Harassment Act is generally cited as the “cyberstalking law.” Although the statute covers both threats and harassment, 47 U.S.C. § 223 applies only to direct communications between the

dead.”); See infra note 82 for more on the possibility of male-dominated Internet culture as a result of the dog-eat-dog mentality that many programmers espouse.

Press Release, Working to Halt Online Abuse, Oldest Online Organization Discusses Current Cyberstalking Statistics (Mar., 2010) (available at http://neterimes.livejournal.com/186367.html). Notable statistical findings include: Single victims increased in 2009 from 31.5% to 43% and married victims showed an increase from 18.5% in 2008 to 27% in 2009; Victims who knew their harassers in 2009 showed an increase of 4% over 2008, and family members and students jumped in numbers as harassers; as in previous years, the initial harassment began via e-mail first, no matter where they may have encountered their harasser (if they did). Id; see also S. Aggarwal, P. Henry, L. Kermes, & J. Mulholland, Evidence Handling in Proactive Cyberstalking Investigations: The PAPA Approach, 2005 PROC. OF THE FIRST INT’L WORKSHOP ON SYSTEMATIC APPROACHES TO DIGITAL FORENSIC ENGINEERING 165 (discussing new developments in data collection within the cyberstalking context).


Id.


perpetrator and the victim. It would not reach a cyberstalking situation where a person victimizes another person by posting messages on a bulletin board or in a chat room impersonating them or soliciting acts of violence against them. Moreover, § 223 is only a misdemeanor, punishable by not more than two years in prison.

3) The Interstate Stalking and Prevention Act, as amended by VAWA

The Interstate Stalking and Prevention Act, initially signed into law by President Clinton in 1996, makes it a crime for any person to travel across state lines with the intent to injure or harass another person if in the course thereof, the perpetrator places that person or a member of that person's family in a reasonable fear of death or serious bodily injury. A number of serious stalking cases have been prosecuted under § 2261A, but the requirement that the stalker physically travel across state lines makes it largely inapplicable to cyberstalking cases.

4) 18 U.S.C. § 2425

President Clinton signed this bill into law in October 1998, making it a federal crime to use any means of interstate or foreign commerce (such as a telephone line or the Internet) to knowingly communicate with any person with the intent to solicit or entice a child into unlawful sexual activity. This may help target specific occasions of cyber solicitation, but not only is it limited to children, it is limited to “harassing phone calls to minors . . . showing intent to entice or solicit the child for illicit sexual purposes,” which highly constricts its applicability.

Other countries have begun to include online abuse in their anti-stalking legislation. In Australia, the Stalking Amendment Act (1999) includes the use of any technology to harass a target as a form of criminal stalking, while in the United Kingdom, the Malicious Communications Act (1998) classifies cyberstalking as a criminal offense.

---

27 Id.
29 In United States v. Bowker, 372 F.3d 365, 21–23 (6th Cir. 2004). Bowker was convicted under § 2261A and sentenced to eight years in prison after he sent obscene e-mails, made threatening telephone calls, and stole mail from the victim. The victim was a TV reporter in West Virginia; the defendant resided in Ohio.
D. Problems with Cyberstalking Statutes

1. How kinetic must the harm be?

The work to create statutes addressing cyberstalking reflects the difficulty in defining the harm: fear as a harbinger of potential future physical harm, or fear or harassment as a harm in and of itself. Thus, on one side are statutes that “criminalize certain acts of harassment in order to prevent more serious violent conduct by the stalker.” This corresponds to the search for manifestations of kinetic-world harm. On the other side is a recognition that stalking has “a profound effect upon the victim” and “generally, the goal of a stalker is to exert ‘control’ over the victim by instilling fear in her.” This second view corresponds to a recognition that cyberstalking harms do not require a physical manifestation to be real.

2. Problems with both “credible threats” doctrine and the “reasonable person” standard

Over one-third of state stalking statutes have a credible threat requirement. Generally, a credible threat is “a verbal or written threat” coupled “with the apparent ability to carry out the threat” so as to cause the victim fear.

As I have described, I find the impulse to look for physical harm to be myopic and problematic as the basis for a legal standard. Further, the analysis of a threat’s credibility may be warped in the cyber context, because “how real” a threat is traditionally revolves around access to the victim; but in the cyber context, someone could enact great harm from a distance. In one case, a cyberstalker (whose victim had repeatedly spurned his romantic advances) terrorized his victim by impersonating her in various Internet chat rooms and posting her telephone number and address, with messages that she fantasized of being raped. In response to the messages, at least six men on separate occasions knocked on the woman’s door saying that they wanted to rape her. The “credible threat” component is almost impossible to assess in the cyber context—it is impossible to know how real a threat is without the benefit of hindsight. And as this example shows, the solicitation of third-party stalkers seems to be a loophole that the “credible threat” legal doctrine statutes do not acknowledge.

In another case, a cyberstalker posed as his victim and sent hate e-mail, including her real name, telephone number, and address and while painting her as a Satanist, drug user and pornographer. She only learned of this when she received a phone call from a
man in response to her alleged racist statements online. The man, who happened to live a mere twenty minutes from her, said on the phone, “You’d better get a gun because the next time we read about you it will be in a police report.”39 This cyberstalker’s behavior certainly seems to have resulted in a “credible threat” but because the cyberstalker had not been the one to threaten her directly, the victim had no criminal recourse.

Moreover, this unique cyberstalking scenario reflects another hole in the “credible threat” doctrine: the ability to impersonate a victim online. As Professor Goodno states, “Unlike offline stalking, the cyberstalker can easily take on the identity of the victim and create havoc on-line. The cyberstalker, pretending to be the victim, can send lewd e-mails, post inflammatory messages on multiple bulletin boards, and offend hundreds of chat room participants.”40 The ability to impersonate a victim creates new dynamics of abuse—and a criminal prosecution may not be able to reverse the wounds to reputation.

In light of problems with the “credible threat” standard, many have advocated a “reasonable person” standard instead.41 According to the reasonable person standard, the determining factor triggering prosecution is whether the perpetrator’s conduct would cause a reasonable person to fear for his or her safety.42 The reasonable person standard recognizes that the crime of cyberstalking (and its associated hurt) is defined by the victim’s subjective experience of fear.43

I support a statutory scheme that recognizes that fear, which may also be the anticipation of future hurt, is a form of harm in itself. In fact, the latest numbers from Working to Halt Online Abuse show that even while online abuse climbs steadily, “[a]buse threats of offline violence dropped from 25% to 16.5% in 2009.”44 But how ought we measure fear as a harm? If fear is evaluated in light of the “reasonable person” standard, to what extent is the reasonable person in the eye of the victim and to what extent in that of the stalker?

The victim’s fear might hinge on who the stalker is. The level of fear might be different if one is stalked by an ex-boyfriend, a stranger, a fan, or by a group of people. Fear level might also differ based on the cyberstalker’s characteristics: an ex-con

40 Goodno, supra note 14, at 137; see also infra Part III (discussing how the stake we have in our online identity both overlaps and exists independently of our offline identity).
41 See, e.g., Goodno, supra note 14, at 146 (“[S]tatutes which have a credible threat requirement—either those that have attempted to incorporate cyberstalking in preexisting statutes or those that have been specifically targeted at cyberstalking—cannot fully address all aspects of cyberstalking. This is because they focus on the cyberstalker’s conduct. The reasonable person standard, however, is better in cyberstalking cases because it focuses on the fear that the cyberstalker intentionally meant to instill in his victim.”).
42 See, e.g., DEL. CODE ANN. tit. 11 § 1312(a) (2010).
43 The trigger for prosecution under DEL. CODE ANN. tit. 11 § 1312a is whether the perpetrator’s conduct “would cause a reasonable person to fear . . . physical injury to himself or herself . . . .” Id. The reasonable person standard purports to be more sensitive to victims’ protection because the credible threats standard is a purely “objective” standard whereas the reasonable person standard is an “objective” standard based on a “subjective” experience of fear. However, because the reasonable person standard revolves around fear that “we” recognize as a society, in practice it seems necessarily to weave between whether we think a person in this position would feel fear, and whether we think this person in this position feels fear.
stranger, an ex-spouse with violent tendencies, or an acquaintance with sophisticated hacking skills. Goodno advocates a reasonable person standard on the grounds that “[s]tatutes that are most useful and successful in prosecuting cyberstalkers and protecting victims are those which shift the focus from the perpetrator’s behavior to the effect on the victim.”45 In reality, the reasonable person standard seems not much easier to implement than the credible threat standard, as enforcement still depends upon some form of social meter even if allegedly based on the victim’s “subjective” experience of fear. Because we cannot—and would not want to—say that ex-convicts or ex-boyfriends have a diminished First Amendment right (even though they might inspire more fear in their stalking victims), one area of myopia seems to be the law’s inability to recognize different people are capable of enacting different forms of harm. First Amendment rights constantly weigh against the reasonable person standard.

II. **CYBERSTALKING STATUTES AND THE FIRST AMENDMENT**

Any attempt to criminalize cyberstalking will come up against a First Amendment objection. Because a restriction on cyberstalking as speech would necessarily be content-specific, it would come under strict scrutiny, and the constitutionality of the restriction is likely to be upheld only if it falls within one of the delineated exceptions.

There has always been some speech that has been unprotected; today, categorically unprotected speech includes hate speech, sexual harassment, and child pornography. Even categorically unprotected speech usually falls within an accepted rationalization for First Amendment abridgement: criminal threats and low-value speech. First Amendment jurisprudence over the decades seem to have varied based on the particular fears of the day—revolving not just around the question of regulation versus freedom, but who and what is regulated, what it opens the door for in the future, what the grounds for regulation are, and who is making the determination to regulate.

¶ 1

A. **Accepted Rationales for First Amendment Abridgements**

The specific justifications for abridging First Amendment rights to prosecute cyberstalking will depend on what the statements are—if it is a threat, it submits to the criminal threats framework; if not, it must be brought under some version of low-value speech justifications.

1. **Criminal Threats, Hate Speech and “Fighting Words”**

If the cyberstalking takes the form of threats, the outcome of a claim regarding a criminal threat depends on the content of the speech itself (including whether it is directed at one individual, whether that individual is the President, etc.), as well as the Court’s chosen standard addressing imminence and depth of the harm threatened. If the cyberstalker is threatening a particular and tangible harm (i.e. to injure or kill a particular person), this speech would be considered a greater danger. If the stalker is proposing a

---

generalized and intangible harm (e.g. condemnation of lifestyle or expressed frustration with lack of reciprocity in a relationship), this speech will be more difficult to prosecute based on the “fighting words” doctrine.

A claim to a First Amendment threat, or “fighting words,” exception depends on the standard that the Court employs, including whether they choose to use a Brandenburg “imminence” test to assess the harm, or whether non-imminent threats are sufficiently dangerous. If the cyberstalker’s speech is more expressive than a “call to action,” it is much less likely to qualify as unprotected. The Court has maintained a fairly strict test for menacing speech to fall within the unprotected realm. In *NAACP v. Claiborne Hardware*, 458 U.S. 886, 902 (1982), the Court upheld the constitutionality of menacing speech uttered in a context of some violence, and as thinly veiled as “if we catch any of you going in any of them racist stores, we’re gonna break your damn neck.” In *Planned Parenthood v. American Coalition of Life Activists*, 244 F.3d 1007 (9th Cir. 2001), the Ninth Circuit reversed a ruling punishing a website entitled the *Nuremberg Files* that espoused violence against pro-choice politicians, abortion providers, and other pro-choice activists. It included lists of photographs and locations (home and work addresses) of people whom the American Coalition of Life Activists had targeted as “war criminals” as well as lists of those already killed or wounded. Neither the openness of the threats in *NAACP v. Claiborne Hardware*, nor the nastiness of the ACLA’s mission, was enough to move the menacing words out of the realm of protected speech. There are many who advocate a shift in standards to accommodate Internet safety interests more effectively, but so far the imminence standard is still relevant.

47 See, e.g., Boucher v. School Bd. of the School Dist. of Greenfield, 134 F.3d 821, 828 (7th Cir. 1998). (Expulsion of a student who published an article about ‘hacking’ the school’s computer system in an underground newspaper upheld because the Seventh Circuit held he was making a “call to action detrimental to the tangible interests of the school”).

Not all stalkers meet the criteria for any specific or serious psychiatric disorder. However, some of the most extreme and dangerous stalkers are those fueled by a mental illness. Primary diagnoses for mentally ill stalkers include schizophrenia, bipolar disorder, or a delusional disorder. Some stalkers have personality disorders (identified by a pervasive abnormal pattern of behavior related to thinking, mood, personal relations, and impulse control). Specifically, these stalkers have antisocial, borderline, histrionic, narcissistic, dependent, or obsessive-compulsive personality disorder characteristics. Substance abuse and/or dependence frequently are contributing factors.

Most often, Kulbarsh writes, “the less of a relationship that actually existed between the victim and stalker prior to the stalking, the more mentally disturbed the stalker is.”
2. Low-Value Speech

If not a threat, the other avenue to exemption from First Amendment protection is low-value speech. One concrete example of this is obscenity. The rationale for excluding obscenity is either concerns about “poisoning of the mind” or dubious claims that speech like pornography (and religious speech) is so evocative as to constrict rational thought and take over rational powers of thought and speech.51 Cyberstalking does not easily fit this rubric; if one only looks at an isolated communication, it can be innocuous. Also within the low-value exemption from First Amendment protection is child pornography. Child pornography regulations may be a unique analog to cyberstalking regulations in that part of the justification is a harm itself.52 But because of child pornography’s unique criminalization rationale that every time the image is viewed, the child is “re-violated,” it seems highly unlikely to be helpful to apply the framework to cyberstalking. An act of cyberstalking is not criminal in isolation as child pornography is. Rather, a single incidence of cyberstalking—which would be an unwanted communication or posting online—is not only legal but central to the core of the First Amendment. Cyberstalking a celebrity, especially if that person has a political bent to him/her or if the stalker has a political bent to his communications, could become even closer to the “core” of First Amendment protection, political dissent.53

Application of First Amendment doctrine seems perverted in the cyberstalking domain, especially if nonconformist speech falls under the “political speech” core. The Supreme Court has historically protected non-traditional political speech: flag flying and flag burning cases usually revolve around the question of whether it ought to be suppressed for its content as a symbol, either sacred or sacrilegious, or that it cannot be suppressed precisely because of its content as a form of dissident or political speech.54

3. General Overview of the Court’s Trajectory

Until the 1970s, the only speech that was suppressed was that which could be traced to a tangible harm. According to Justice Holmes in Schenck v. United States, 249 U.S. 47, 52 (1919), a “clear and present danger” would justify regulation since “the most stringent protection of free speech would not protect a man in falsely shouting fire in a theatre and causing a panic.”55 However, after the 1970s the focus turned from political speech said to cause tangible harms to a different issue: relative value of the speech and intangible harms. After the 1970s, the Court was willing to simply find some speech so low-value as to be worthless.56 In addition, in Reynolds v. United States, 98 U.S. 145

54 The problem with applying the low-value speech framework to cyberstalking is accentuated considering that the Court’s favored response is “counterspeech”—consider, for instance, Justice Brandeis’ admonishment in Whitney v. California, 274 U.S. 357, 377 (1927): “the remedy to be applied is more speech, not enforced silence.” How, exactly, would more speech help in a cyberstalking situation?
55 “Clear and present danger” was coupled with the “bad tendency” test of Whitney, and both were replaced in 1969 by Brandenburg, introducing the “imminent lawless action” test.
56 In Chaplinsky v. New Hampshire, 315 U.S. 568, 571–72 (1942), the Court provided a foundation for considering some speech as valueless:
(1878), the Court had held that the government may regulate speech based on generalized intangible harm and low value. In and after the 1970s, the Court seized on these to expand proscriptions and the government began tolerating a good deal of regulation.

Around the time that Justice Kennedy joined the Court in February 1988, the Court began to focus its regulation on groups who had been and were still disadvantaged—racial and ethnic minorities, religious minorities, sexual orientation minorities, and women. This is when many of the debates about regulation of depictions of types or groups of persons arose, including pornography 57 and “bias-motivated” speech. 58 In R.A.V. a teenager burned a cross on the lawn of an African-American family and was convicted under the St. Paul Bias-Motivated Crime Ordinance prohibiting “plac[ing] on public or private property, a symbol, object, appellation, characterization or graffiti, including, but not limited to, a burning cross or Nazi swastika, which one knows or has reasonable grounds to know arouses anger, alarm or resentment in others on the basis of race, color, creed, religion or gender.” 59 Justice Scalia for the majority ruled the St. Paul ordinance constitutionally overbroad because “The First Amendment does not permit St. Paul to impose special prohibitions on those speakers who express views on disfavored subjects.” 60 It was precisely the controversial nature of this “point of view” that Scalia contended made it political speech and therefore protected.

While we as a society are increasingly willing to recognize stalking and cyberstalking as legitimate threats, the Court remains in the post-70s mode of fearing or just disliking the idea of a “thought police” (in Scalia’s terms, the fear that “official suppression of ideas is afoot.”). 61 This may undergo a shift, especially in the Internet crime context, as it becomes clear that (1) even when the Court claims to or aspires to refrain from content regulation, it is clear that it espouses certain societal values that are reflected in our First Amendment protections, and (2) it would be hard to argue that those engaging in cyberstalking speech are a suppressed class in need of protection, considering their potential power to damage. In contrast, it is fairly easy to demonstrate that those victimized by cyberstalking may be a class in need of protection. 62

On top of this, general distaste for regulation may factor in—just as Judge Easterbrook in Hudnut claimed that even if all of the alleged harms of pornography are true, we still ought not to regulate it because attempts to regulate only exacerbate the issue. 63 In the case of stalking, one could argue that attempts to regulate would formally acknowledge the power of stalkers, in a sense enfranchising them through our very fear. Since the goal of stalking may be nothing more than a sense of power or attention, one

---

57 American Booksellers Ass’n v. Hudnut, 771 F.2d 323 (7th Cir. 1985), aff’d, 475 U.S. 101 (1986).
59 Id. at 380.
60 Id. at 391.
61 Id. at 390.
62 See infra Part III for more on the disturbing patterns of cyberstalking victims’ characteristics.
63 Judge Easterbrook writes, “…an idea is as powerful as the audience allows it to be.” American Booksellers Ass’n, 771 F.2d at 327–28.
could argue that enacting legislation criminalizing stalker speech will only serve to legitimize or formalize their presence in our society. As Schwartz wrote in “The Trolls Among Us,” “trolling will stop only when its audience stops taking trolls seriously.”

On a more abstract level, cyberstalking may resemble a “speech act” more than mere speech (perhaps this is another reason why we crave a physical manifestation of the harm). But the legal parameters defining what speech qualifies as a speech act are circumscribed and it is unlikely that cyberstalking would qualify, especially since cyberstalking is even more “purely” a First Amendment issue than kinetic-world stalking—which could include some combination of acts that do not closely resemble speech, such as in-person encounters or surveillance, or even just breathing into a phone.

4. Internet as a Forum

I have focused on criminal aspects of cyberstalking enforcement. There is a potential for civil enforcement; because of lower burdens of pleading and a general difficulty in proving criminality of the behavior, civil action seems to be a good option. According to one lawyer’s website, “[p]rotecting yourself against [cyberstalking] is difficult since typically the behavior is not clearly illegal and the police often don't take the problem seriously. As a practical matter, I think that you might have better luck with the police if you reported aliens landing in your backyard.” Liability for Internet Service Providers (ISPs) is one proposition for civil enforcement; however, section 230(c)(1) of the Communications Decency Act of 1996 provides broad immunity for ISPs for any content on their sites. This disincentivizes providers from learning what is on their site, and makes it impossible to prosecute ISPs once harmful content is discovered. Even if restrictions were strengthened, as has been advanced in the past, foreign sites would be unaffected.

III. NOT ALL ARE CYBERSTALKED EQUALLY

As I have described, cyberstalking is a significant problem, yet difficult to pinpoint legally—a thorny combination. But perhaps the darkest side of this underbelly of the open Internet is the fact that cyberstalking happens disproportionately to certain people or groups of people. The numbers support what we may know anecdotally to be true: according to a 2006 study, individuals writing under female names received twenty

---

64 Schwartz, supra note 16.
five times more sexually menacing comments than posters writing under male names.\textsuperscript{69} Working to Halt Online Abuse reports that in 2006, 70\% of the 372 individuals that it helped combat cyber harassment were female, and in half of those cases, the victims had no connection to their stalkers.\textsuperscript{70} One lawyer’s website explicitly counsels people to “prevent” cyberstalking by changing their emails and profiles to remove all female gender-identifying information because “Jdoe@CompuServe.com is a less likely victim than JaneDoe@CompuServe.com . . . The simple reality is that females are the usual targets of both stalkers and cyberstalkers.”\textsuperscript{71} The idea that changing one’s username “prevents” cyberstalking seems misleading—it does not get at the root of the problem, and may in fact buy into cyberstalker mentality.

A. Patterns of Online Abuse

1. Unlike cancer, cyberstalking is a social disease

The social patterns of victimization distinguish cyberstalking from other cyber scourges, and show it to be especially sinister. In a personal interview on the topic of cyber security, Bob Giesler, Vice President for Cyber Programs at SAIC, urged me to “think about [cyber insecurity] as a cancer . . . you already have it, it’s hard to detect, it may be fatal but it’s also treatable.”\textsuperscript{72} An organic metaphor may be a useful characterization of cyber insecurity generally, but it is not an apt analogy for cyberstalking; cyberstalking is a communal problem precisely because it is a problem that affects certain individuals unequally. Unlike botnets and credit card fraud, the crime of cyberstalking forces us to face the proposition that life online as a woman is different than life online as a man. Our statutes attempt to address systematic discrimination in the kinetic world, but they seem to be failing in the online world, at least in the cyberstalking dimension.

Kathy Sierra was a rising star in the tech world when cyberstalkers repeatedly attacked her blog, including death threats, and she had to shut it down out of fear.\textsuperscript{73} One blog post included an image of Sierra next to a noose. As she related her decision to shut down the blog, Sierra wrote: “I have cancelled all speaking engagements. I am afraid to leave my yard, I will never feel the same. I will never be the same.”\textsuperscript{74} A common legal standard for a claim of sexual harassment is whether the behavior “would not have occurred but for her sex.”\textsuperscript{75} Sierra’s case certainly seems to fit. In the wake of the threats

\textsuperscript{69} Michel Cukier and Robert Meyer, Assessing the Attack Threat due to IRC Channels, http://www.enre.umd.edu/content/rmeyer-assessing.pdf (last visited Apr. 29, 2010).
\textsuperscript{70} Working to Halt Online Abuse, 2006 Cyberstalking Statistics, http://www.haltabuse.org/resources/stats/index.shtml. That such a high proportion of cyberstalkers were strangers suggests that it is a societal-level problem.
\textsuperscript{71} Grossman, supra note 65.
\textsuperscript{72} Telephone interview with Bob Giesler, Vice President for Cyber Programs, Science Applications International Corporation (Jan. 5, 2010).
\textsuperscript{75} Bowen v. Dept. of Human Servs., 606 A.2d 1051, 1053 (Me. 1992).
against Sierra and her decision to shut down her blog, peer technology blogger Robert Scoble announced that he removed the function permitting visitors to comment anonymously because “[i]t’s this culture of attacking women that has especially got to stop.”\textsuperscript{76} According to Scoble, “[W]henever I post a video of a female technologist there invariably are snide remarks about body parts and other things that simply wouldn’t happen if the interviewee were a man.”\textsuperscript{77} While our kinetic-world standards attempt to recognize systematic patterns of treatment, for some reason it seems that our moral or legal red flags do not go up when we witness it—or experience it—online.

In a sense, it is ironic: all of the factors that could have socially liberated Internet culture (anonymity, geographic overlap, ability to find those who share a quirky personal interest) seem to have become those that most socially threaten. Cyberstalking is one powerful example of this. In 1993, the Harvard Journal of Law and Technology held their annual symposium on “Electronic Communications and Legal Change.”\textsuperscript{78} The impetus for the topic, according to the program, was the “exciting” notion that “electronic mail removes the visual cues that identify people by race, age, gender or other similar classification.”\textsuperscript{79} The naïve hopefulness of the program’s tone is telling.\textsuperscript{80} The language shows promise; upon reflection, that hope for transcending kinetic patterns of abuse seems logically justified—but as we know, the promise has been largely betrayed.\textsuperscript{81}

---

\textsuperscript{76} Sierra, supra note 73.

\textsuperscript{77} Id.


\textsuperscript{79} Id. at 213. The report continues, “This ‘leveling’ effect offers the potential of creating an electronic forum for allowing open discussion of otherwise sensitive issues.” Id.

\textsuperscript{80} In a similar trajectory, a 1996 article in the N.Y.U. Law Review celebrated the Internet as the herald of a new dawn of self-publishing that would level the playing field for less-established academics. Bernard Hibbitts Last Writes? Reassessing the Law Review in the Age of Cyberspace, 71 N.Y.U. L. REV. 615 (1996). Exactly 10 years later, in the Yale Law Review Rosa Brooks answered him (though without acknowledging and presumably without intending as such) in her piece What the Internet Means for Female Scholars, concluding simply:

[V]ery few commentators have focused on the gender impact of the Internet on female academics. (Perhaps in part this is because most of those who write about the effect of Internet technologies on law are men—last spring, for instance, Harvard Law School’s Berkman Center on the Internet and Society brought together prominent legal bloggers—mostly law professors—to look at ‘how blogs are transforming legal scholarship.’ Nearly three-quarters of the panelists were men.)


Thus, while the Internet may eliminate some of the felt pressure to attend conferences and publish long pieces—which affect women disproportionately because they tend to be the primary child care-giver—the Internet age may also bring new dangers for women in the legal academy. Indeed, the online world of legal scholarship may ultimately replicate many of the hierarchical and gendered structures found in the offline world of legal scholarship.” Id. at 50.

\textsuperscript{81} I wonder if part of the limits of the Internet as a great equalizer is its inherent fetishization of the “cutting-edge,” which in the end may be a quite limiting proposition. Scholars like Jonathan Zittrain advocate for a wide-open Internet landscape with lots of “generativity.” See generally JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT (Yale University Press, 2008). But how many people are really participating in the generativity aspects like code-writing, and what are the demographics of that group of people? Sometimes, the Internet seems to be a haven for the tech-savvy to harass, or at least dominate, the less-tech-savvy. Infamous troll Weev stated this overtly in a phone conversation with Mattathias Schwartz about trolling, calling it “basically Internet eugenics...I want everyone off the Internet.
2. Our stake in our online persona creates new vulnerabilities (for cyberstalkers to exploit)

Cyberstalking power dynamics seem to track somewhat closely—and perhaps even exacerbate—stratification categories in the kinetic world; but I contend that there are new categories emerging too. Certainly, women (and those with female usernames) have tended to attract more hatred online; now, those who are less tech-savvy also may be of particular vulnerability—not only to being ridiculed online, but also to someone hacking their accounts or installing key-loggers—a form of abuse not previously available. One’s online persona stems from new depth of use of the Internet, and these new uses create new vulnerabilities.

I propose that the interest we have in our online persona may overlap with our kinetic-world persona, but it may also have an independent life. This is due in part to the fact that so much has moved online and so many have access to Internet—from prospective employers or mothers-in-law to one’s spouse or high school acquaintance. There is simply no comparison to the kinetic-world, and the notion that one can avoid cyberstalking by “turning off the computer” is unimaginable.

The kinds of things we fear in the kinetic world—being mugged while walking home alone on a dark street, having one’s car stolen from a parking lot—do not map neatly onto the cyber world. Unsurprisingly, the kinds of fears we have online—not just those that are threats in a new forum, but cyber-specific fears such as the possibility that someone may post vicious rumors or Photoshopped pictures that could destroy personal or professional relationships—are in many ways unique. Searching for kinetic-world correlations may be possible but is not necessarily useful.

For these reasons, I find that cyberstalking is a crime distinguished from kinetic-world stalking, and not just an expansion of the stalking location. The kinds of harms one can experience online are different, and this is crucial since the justification for criminalizing cyberstalking (which is, after all, otherwise-lawful speech) is a harm-based model. The current system’s focus on kinetic harm is one of the obstacles to preventing, identifying, and giving tools to fight back against, some of the specific fears that result from cyberstalking (which tend to be less real-world paralleled).

3. Who is harmed by patterns of cyberstalking?

Whether the harm from cyberstalking is to individuals or the collective is an important step of analysis in determining the amount of social harm that arises from cyberstalking. While we all have a general interest in the safety of society, I posit that the harm of kinetic-world stalking is more able to be pinpointed on its victim. The victim is the one who experiences the car driving by her house repeatedly, the heavy breathing phone calls, the black roses delivered at work or the post-it notes on her dashboard. If the stalking is

Bloggers are filth. They need to be destroyed. Blogging gives the illusion of participation to a bunch of retards. . . . We need to put these people in the oven!” Schwartz, supra, note 16.

82 As web designer Clement Mok stated in 2001, “Five years ago the Web was one-dimensional—very much about communication. We thought of it as a new medium, not a new economy.” Darwin Magazine, Mar. 2001, available at http://www.clementmok.com/files/01_Darwin.pdf (last visited Apr. 28, 2010). I contend that in this “new economy,” the reciprocity of interaction as a result of power dynamics—monetary or other—continues to exist, the exchange merely occurs in different ways than it does in the kinetic world.
limited to the physical world, there can be physical isolation of the stalking behavior to the object of its pursuit—while we empathize with victims and we care whether people in our society are victimized in this way, it is a localized kind of harm.

Cyberstalking is not conducted in isolation—on the contrary, cyberstalking behavior changes the landscape on which we all operate online. A cyberstalker posting death threats on a female techie’s blog not only reaches his victim (though he does that), he also reaches every other viewer, those who know her and those who do not, those who identify with her and those who identify with him. According to Schwartz’s account of trolling culture, new trolls form when they witness existing trolls’ behavior and want to “be in on the joke;”83 on the flip side, users who witness aggressive or degrading online behavior seem likely to monitor their own uses of the Web—or even to victimize others in similar ways.

That cyberstalking tracks certain categories of people makes this proposition even more problematic. We don’t need to deal with stalking just to save certain individuals on the fringes who are experiencing this victimization; we need to deal with cyberstalking because it is behavior that inserts itself into our Internet culture, molding the landscape. I do not contend that the harm of cyberstalking is greater than the harm of kinetic-world stalking; it simply seems that there is something different about the way this harm diffuses into the world.

IV. CONCLUSION: WHERE DO WE GO FROM HERE?

Cyberstalking is a complicated problem, and facing it is inconvenient because it cannot be addressed neatly within existing legal frameworks (in fact, in the context of the First Amendment in particular, it challenges them quite directly). Moreover, those enacting or enforcing statutes (predominantly middle-aged white men) are unlikely to be the same people who experience cyberstalking, nor might we expect them to feel especially high levels of fear in response to cyberstalking behavior.84 This calls into question suggestions like Orin Kerr’s reassurance that we rely heavily on prosecutorial discretion to administer a new cyber statute that some contend is too broad: “[T]he text looks really broad, but prosecutors know that they can’t bring a prosecution unless doing so would comply with the Supreme Court’s First Amendment cases.”85 Kerr’s reliance on prosecutorial discretion is hard to subscribe to considering the circles of influence in

83 Schwartz, supra note 16 (“If you don’t fall for the joke, you get to be in on it.”).
84 When in an unfortunate twist of events a female Ropes and Gray partner became the victim of a cyberstalker, she was able to hire a public relations team to combat the lies he was posting, and to prosecute him publicly; even though the cyberstalker fled to Europe, the damage to her reputation was salvaged. Lukey’s (the victim) experience so disturbed her, she has even drawn up new cyberstalking legislation. See Tormented by Cyberstalker, Ropes Partner Drafts New Legislation, AM LAW DAILY, Apr. 17, 2009, available at http://amlawdaily.typepad.com/amlawdaily/2009/04/ropes-gray-partner-fights-cyberstalker.html. Of course, most people do not have the resources to wage a war like Lukey did—but her reaction suggests that if more people in positions of legal authority experienced direct victimization, they might be spurred to act and the statutory landscape might look different.
the world, and prosecutorial discretion adds another dimension to the fact that law is a blunt instrument to deal with cyberstalking.

Cyberstalking raises foundational legal questions that will recur. I submit that we must confront these questions with the recognition that the Internet is not merely a new medium for speech; it is a space in which actions occur. Creating effective cyberstalking statutes will force us to think about where we want the limits of free speech online, and how well we understand the kinds of harms that exist on and because of the Internet. 86 Letting go of our attachment to kinetic manifestations of harm and deciding upon standards for aggressive online behavior means that there will be trade-offs when it comes to making and enforcing cyberstalking laws. There is no perfect solution. But I believe we can make those trade-off decisions deliberately, informed by values we choose to live by as Internet citizens. 87

In a law enforcement dimension—that is, treating the current cyberstalking activity—I contend that we ought to acknowledge online harms more cogently as we make decisions about where we want to draw legal lines. Of the deeper, cultural dimension—the base question as to why there are these patterns of online abuse and what to do to staunch the flow—I ask, in Luce Irigaray’s words, “Can we speak, can we speak to each other differently?” 88 To my mind, there is some promise for injecting a counter to the Internet culture of inequality by creating legal resort—just as the evolution of laws changed the culture of workplaces and schools. 89

---

86 I recognize that cyber-specific laws would have their down-sides; Congress is not known for being tech-savvy, and technology can change to make the definitions outdated before the law is even released. But I advocate laws that would at least recognize the kinds of activity going on online, the stake one has in one’s online persona, and the fears we experience online. To create a cyberstalking approach in the law, we must be willing to delve into the dark underbelly of unique harms that arise online and establish values by which we will live in the Internet world.

87 I use the term “citizen” deliberately to connote the legal aspects of participation in a society as well—as philosopher Jürgen Habermas writes, citizenship produces “abstract, legally mediated social integration.” JURGEN HABERMAS, THE INCLUSION OF THE OTHER, STUDIES IN POLITICAL THEORY 159 (MIT Press, 1998).

88 PETER J. BURGARD, NIETZSCHE AND THE FEMININE 329 (University of Virginia Press, 1994). Irigaray continues, “Would this not be the dawn of the new era? For no matter where we run to, unless we change the code, the imperatives of the computer will catch up with us.” Id. Cultural shifts are subtle and difficult to manipulate, and will take many angles of work—from bloggers identifying problematic treatment of fellow bloggers to the diversity of computer-savvy people expanding via education and experience. Given that the next generation of adults will have grown up with the Internet from childhood, I have faith that the demographics of the computer-savvy are moving in the direction of more, and not less diversity—which hopefully will help augment current hacker culture. I note that this is not reducible to a gendered problem—as Irigaray admonishes, “the war is not between the sexes, but between the sons and their shadows.” Id. at 331.

This is not to say that contrarian speech should be outlawed; it is to say that we should pay attention to how open our open Internet really is, and who has the right to participate online without paying some price. We need the right remedies for cyberstalking and other crimes of Internet-introduced harm, to work toward (re)constructing an Internet landscape that avoids the Hobbesian aspects of the one we have created.