



**University of Maryland School of Law
Legal Studies Research Paper
No. 2008 - 41**

Cyber Civil Rights

Danielle Keats Citron



This paper can be downloaded free of charge at:
The Social Science Research Network Electronic Paper Collection
<http://ssrn.com/abstract=1271900>

CYBER CIVIL RIGHTS

DANIELLE KEATS CITRON*

INTRODUCTION	62
I. ANONYMOUS MOBS OF THE TWENTY-FIRST CENTURY.....	68
A. <i>The Destructive Nature of Online Mobs</i>	69
B. <i>The Dynamics of Mob Behavior</i>	81
II. THE COMPONENTS OF CYBER CIVIL RIGHTS STRATEGY	84
A. <i>Converging the Interests of the Majority with Those of Subjugated Groups</i>	85
1. Broader Societal Harm Wrought by Online Mobs	85
2. Traditional Tort and Criminal Laws That Should Be Invoked to Combat Cyber Harassment.....	86
B. <i>A Crucial Deterrent and Remedy for Cyber Harassment of Vulnerable Individuals: Civil Rights Law</i>	89
1. Common Civil Rights Doctrines	91
2. Civil Rights Doctrines Focusing on Anonymous Attackers....	94
III. PROTECTING ONLINE DIALOGUE.....	96
A. <i>Online Mobs and Individual Autonomy</i>	98
B. <i>Civil Rights and the Theory of Free Speech Online</i>	98
1. The Expression-Action Distinction on the Internet	100
2. The Values the First Amendment Protects	102
3. The Inadequacy of Private Responses	104
4. The Extent of Interference with Protected Expression	106

* Associate Professor of Law, University of Maryland School of Law. I owe special thanks to Taunya Lovell Banks, Robert Kaczorowski, Dan Solove, David Super, and Greg Young whose insights proved indispensable to the piece. This Article also benefited from the thoughtful comments of Ann Bartow, Richard Boldt, Karen Czapanskiy, Laura DeNardis, Martha Ertman, Lisa Fairfax, Jim Fleming, Susan Freiwald, Nathaniel Gleicher, Mark Graber, David Gray, James Grimmelman, Debbie Hellman, Chris Hoofnagle, Sherrilyn Ifill, Frederick Lawrence, Brian Leiter, Dan Markel, Bill McGeeveran, Leslie Meltzer, Helen Norton, Martha Nussbaum, Paul Ohm, Frank Pasquale, Rob Rhee, Neil Richards, Jay Stanley, Sonja Starr, Cass Sunstein, Chris Wolff, Diane Zimmerman, Jonathan Zittrain and the participants in Yale Law School's 2007 *Reputation Economies in Cyberspace* symposium, the 2008 George Washington Law-Berkeley Law *Privacy Law Scholars* conference, the 2008 *Computers, Freedom, and Privacy* conference, the Yale Law School Information Society Project's Speaker Series, the University of Chicago's *Speech, Privacy, and the Internet* conference, Fordham University School of Law's Center on Information Policy workshop, the International Network Against CyberHate Global Summit on Internet Hate, the University of Maryland Junior Faculty Workshop, and Professor Jonathan Zittrain's *Cyberlaw* class at Harvard Law School. I also am indebted to my superb editor Lauren O'Leary and her cohorts at the Boston University Law Review. Elise Gelinas, Alice Johnson, Geoff Kravitz, and Susan McCarty provided superb research assistance.

C. <i>First Amendment Doctrine</i>	107
1. Criminal and Tort Law	107
2. Civil Rights Law	111
IV. THE ROLE OF WEBSITE OPERATORS.....	115
A. <i>Should Website Operators Have Immunity?</i>	118
B. <i>On What Bases Should Website Operators Be Liable?</i>	122
CONCLUSION.....	125

Social networking sites and blogs have increasingly become breeding grounds for anonymous online groups that attack women, people of color, and members of other traditionally disadvantaged classes. These destructive groups target individuals with defamation, threats of violence, and technology-based attacks that silence victims and concomitantly destroy their privacy. Victims go offline or assume pseudonyms to prevent future attacks, impoverishing online dialogue and depriving victims of the social and economic opportunities associated with a vibrant online presence. Attackers manipulate search engines to reproduce their lies and threats for employers and clients to see, creating digital “scarlet letters” that ruin reputations.

Today’s cyber-attack groups update a history of anonymous mobs coming together to victimize and subjugate vulnerable people. The social science literature identifies conditions that magnify dangerous group behavior and those that tend to defuse it. Unfortunately, Web 2.0 technologies accelerate mob behavior. With little reason to expect self-correction of this intimidation of vulnerable individuals, the law must respond.

General criminal statutes and tort law proscribe much of the mobs’ destructive behavior, but the harm they inflict also ought to be understood and addressed as civil rights violations. Civil rights suits reach the societal harm that would otherwise go unaddressed and would play a crucial expressive role in condemning online mob activity. Acting against these attacks does not offend First Amendment principles when they consist of defamation, true threats, intentional infliction of emotional distress, technological sabotage, and bias-motivated abuse aimed to interfere with a victim’s employment opportunities. To the contrary, it helps preserve vibrant online dialogue and promote a culture of political, social, and economic equality.

INTRODUCTION

New technologies generate economic progress by reducing the costs of socially productive activities. Unfortunately, those same technologies often reduce the costs of socially destructive activities. Our legal system depends upon naturally occurring costs to deter much anti-social behavior.¹ A

¹ Thus, the economic inefficiency of wrong-doing, rather prosaically, should join morals, religion, and law on Dean Pound’s list of the “major agencies of social control.” ROSCOE POUND, *SOCIAL CONTROL THROUGH LAW* 18 (Transaction Publishers 1997) (1942)

reduction in these costs often requires extending law to new classes of behavior.

Technology minimizes the costs of pro- and anti-social behavior through two opposing types of changes. Technology disaggregates. Communication advances allow people to separate their ideas from their physical presence. This is equally true for the scientist, the venture capitalist, and the criminal. At the same time, technology aggregates. Transportation advances allow a business to collaborate with far-flung strangers in various states. These same advances allow a computer hacker and a financial whiz to form a more efficient identity-theft ring and to permit terrorists to strike from afar.² Better communications allow researchers in one place to advance a concept conceived in another, but they also allow a criminal in one place to send directions on bomb-making to another who has obtained materials from somewhere else. The challenge for law is to foster positive applications of technology's disaggregative and aggregative potential while understanding and checking as many of its destructive applications as possible.

An anti-social behavior that commonly results from technological and economic progress is civil rights abuse. As communication, travel, and trade become cheaper, and as specialized information becomes easier to transmit, people become freer to specialize in work for which they hold a comparative advantage. Specialization and commodification generate efficiencies, allowing skills to be matched more precisely with work to be done and allowing products to be matched more effectively with demand. They also, however, lead to stratification, alienation, and efforts to extend commodification so far as to threaten humanity and individuality.

For example, this was true when intercontinental land and sea travel allowed the sharing of crops, but also facilitated the slave trade. The Industrial Revolution, and subsequent waves of automation, similarly multiplied economic output while ushering in new means of degrading workers and the environment.³ In our own time, advances in genetics open new doors to bio-medical research and to new kinds of employment discrimination. It is equally true in our cyber age.

The Internet raises important civil rights issues through both its aggregative and disaggregative qualities. Online, bigots can aggregate their efforts even when they have insufficient numbers in any one location to form a conventional hate group. They can disaggregate their offline identities from their online presence, escaping social opprobrium and legal liability for destructive acts.

(explaining that social control is maintained by pressure from our fellow man to uphold civilized society and avoid anti-social conduct).

² Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. (forthcoming 2008) (manuscript at 7, on file with author).

³ Lawrence M. Friedman, *A History of American Law* 360, 364 (3d ed. 2005).

Both of these qualities are crucial to the growth of anonymous online mobs that attack women, people of color, religious minorities, gays, and lesbians. On social networking sites, blogs, and other Web 2.0 platforms, destructive groups publish lies and doctored photographs of vulnerable individuals.⁴ They threaten rape and other forms of physical violence.⁵ They post sensitive personal information for identity thieves to use.⁶ They send damaging statements about victims to employers and manipulate search engines to highlight those statements for business associates and clients to see.⁷ They flood websites with violent sexual pictures and shut down blogs with denial-of-service attacks.⁸ These assaults terrorize victims, destroy reputations, corrode privacy, and impair victims' ability to participate in online and offline society as equals.

Some victims respond by shutting down their blogs and going offline.⁹ Others write under pseudonyms to conceal their gender,¹⁰ a reminder of nineteenth-century women writers George Sand and George Eliot.¹¹ Victims who stop blogging or writing under their own names lose the chance to build robust online reputations that could generate online and offline career opportunities.

Kathy Sierra's story exemplifies the point. Ms. Sierra, a software developer, maintained a blog called "Creating Passionate Users."¹² In early 2007, a group of anonymous individuals attacked Ms. Sierra on her blog and two other websites, MeanKids.org and unclbobism.com.¹³ Posters threatened rape and

⁴ See DANIEL J. SOLOVE, *THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET* 81-82 (2007).

⁵ Jessica Valenti, *How the Web Became a Sexists' Paradise*, *GUARDIAN* (U.K.), Apr. 6, 2007, at 16, available at <http://www.guardian.co.uk/world/2007/apr/06/gender.blogging>.

⁶ See Azy Barak, *Sexual Harassment on the Internet*, 23 *SOC. SCI. COMPUTER REV.* 77, 80 (2005).

⁷ See *infra* notes 49 and 72 and accompanying text.

⁸ Anna Greer, Op-Ed., *Misogyny Bares Its Teeth on Internet*, *SYDNEY MORNING HERALD* (Australia), Aug. 21, 2007, at 15, available at <http://www.smh.com.au/news/opinion/misogyny-bares-its-teeth-on-internet/2007/08/20/1187462171087.html>. Denial-of-service attacks occur when an online group or individual forces a victim offline. See *supra* note 51.

⁹ Ellen Nakashima, *Sexual Threats Stifle Some Female Bloggers*, *WASH. POST*, Apr. 30, 2007, at A1.

¹⁰ *Id.*

¹¹ Mary Sarah Bilder, *The Shrinking Back: The Law of Biography*, 43 *STAN. L. REV.* 299, 327 n.161 (1991).

¹² *Creating Passionate Users*, http://headrush.typepad.com/creating_passionate_users/ (last visited Nov. 24, 2008).

¹³ Don Park's Daily Habit, <http://donpark.wordpress.com/> (Mar. 16, 2008, 17:09) (on file with author); Posting of Zephoria to Apophenia, *Safe Havens for Hate Speech Are Irresponsible*, http://www.zephoria.org/thoughts/archives/2007/03/26/safe_havens_for.html (Mar. 26, 2007, 20:20).

strangulation.¹⁴ Others revealed her home address and Social Security number.¹⁵ Individuals posted doctored photos of Ms. Sierra. One picture featured Ms. Sierra with a noose beside her neck.¹⁶ The poster wrote: “The only thing Kathy has to offer me is that noose in her neck size.”¹⁷ Another photograph depicted her screaming while being suffocated by lingerie.¹⁸ Blogger Hugh MacLeod describes the posters as perpetrating a virtual group rape with the site operators “circling [the rapists], chanting ‘Go, go, go.’”¹⁹

The attacks ravaged Ms. Sierra’s sense of personal security. She suspended her blog, even though the blog enhanced her reputation in the technological community.²⁰ She canceled public appearances and feared leaving her backyard.²¹ Ms. Sierra explained: “I will never feel the same. I will never be the same.”²²

Although in theory anonymous online mobs could attack anyone, in practice they overwhelmingly target members of traditionally subordinated groups, particularly women.²³ According to a 2006 study, individuals writing under female names received twenty-five times more sexually threatening and malicious comments than posters writing under male names.²⁴ The organization Working to Halt Online Abuse reports that, in 2006, seventy percent of the 372 individuals it helped combat cyber harassment were

¹⁴ Greg Sandoval, *Blogger Cancels Conference Appearance After Death Threats*, CNET NEWS, Mar. 26, 2007, http://www.news.com/8301-10784_3-6170683-7.html.

¹⁵ Valenti, *supra* note 5.

¹⁶ Sandoval, *supra* note 14.

¹⁷ *Id.*

¹⁸ Valenti, *supra* note 5. Although MeanKids.org’s site operator initially refused to censor the postings due to his “Own Your Own Words” philosophy, he took down the site after Ms. Sierra expressed distress about them. Posting of Jim Turner to One by One Media, <http://www.onebyonemedia.com/the-sierra-saga-part-1-dissecting-the-creation-of-the-kath> (Mar. 28, 2007, 16:31 EST) [hereinafter Jim Turner].

¹⁹ Jim Turner, *supra* note 18.

²⁰ *Blog Death Threats Spark Debate*, BBC NEWS, Mar. 27, 2007, <http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6499095.stm>.

²¹ *Id.*

²² *Id.*

²³ Posting of Lisa Stone to BlogHer, <http://www.blogher.com/node/17319> (Mar. 27, 2007, 3:47) (explaining that countless women have been threatened with rape, dismemberment, and violent images in online forums such as message boards and blog comments).

²⁴ Robert Meyer & Michel Cukier, *Assessing the Attack Threat Due to IRC Channels*, in PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON DEPENDABLE SYSTEMS AND NETWORKS 467 (2006), available at <http://www.enre.umd.edu/content/rmeyer-assessing.pdf> (finding that individuals with ambiguous names were less likely to receive malicious messages than female users, but more likely to receive them than male users).

female.²⁵ In half of those cases, the victims had no connection to their attackers.²⁶ These mobs also focus on people of color, religious minorities, gays, and lesbians.²⁷

These attacks are far from the only new challenge to civil rights in this Information Age,²⁸ but they are a serious one. Without an effective response to both aggressive, bigoted attacks and to more passive forms of exclusion, online equality is more of a slogan than a reality.

Nonetheless, the development of a viable cyber civil rights agenda faces formidable obstacles. First, because it must fill the gap left when the Internet's disaggregation allows individuals to escape social stigma for abusive acts, the cyber civil rights agenda must be fundamentally pro-regulatory. A regulatory approach clashes with libertarian ideology that pervades online communities.

Second, civil rights advocacy must address inequalities of power. This may seem incongruous to those who believe – with considerable justification in many spheres – the Internet has eliminated inequalities by allowing individuals' voices to travel as far as those of major institutions. This assumption may slow recognition of the power of misogynistic, racist, or other bigoted mobs to strike under cloak of anonymity, without fear of consequences.

Third, a cyber civil rights agenda must convince a legal community still firmly rooted in the analog world that online harassment and discrimination profoundly harm victims and deserve redress. In particular, proponents of cyber civil rights must convince courts and policymakers that the archaic version of the acts-words dichotomy fails to capture harms perpetrated online. The Internet's aggregative character turns expressions into actions and allows geographically-disparate people to combine their actions into a powerful force. Those who fail to appreciate the Internet's aggregative powers may be inclined to dismiss many of the harms, perhaps citing “the venerable maxim *de minimis non curat lex* (‘the law cares not for trifles’).”²⁹ For example, an online mob's capacity to manipulate search engines in order to dominate what prospective

²⁵ WORKING TO HALT ONLINE ABUSE, 2006 CYBERSTALKING STATISTICS 1 (2006), <http://www.haltabuse.org/resources/stats/2006Statistics.pdf>.

²⁶ *Id.*

²⁷ See *infra* notes 54-56, 89, 103, 121-127, 131, 143 and accompanying text.

²⁸ The Internet also confers great opportunities on those with the physical and intellectual capital to aggregate with others who are similarly situated, but in so doing it furthers the disadvantage of those who do not share the same physical and intellectual capital. The “digital divide” resembles the enhanced isolation that pervasive telephone ownership imposes on those who cannot afford and that structured, urban environments impose on the homeless. For an explanation of how the “digital divide” operates, see generally Allen S. Hammond, IV, *The Telecommunications Act of 1996: Codifying the Digital Divide*, 50 FED. COMM. L.J. 179 (1997).

²⁹ See *Wis. Dep't of Revenue v. Wrigley*, 505 U.S. 214, 231 (1992). Courts invoked this maxim to deny relief to those injured at the beginning of the Industrial Revolution. MORTON J. HORWITZ, *THE TRANSFORMATION OF AMERICAN LAW, 1780-1860*, at 71 (1977).

employers learn about its victim, by aggregating hundreds or thousands of individual defamatory postings, may not be grasped by judges accustomed to a world in which defamers' messages either reached a mass audience or were sent specifically to recipients known to the defamer. Much as the northern media initially dismissed the Ku Klux Klan's violence in the early 1870s as "horseplay" borne of "personal quarrels,"³⁰ so have many viewed the destruction wrought by online groups as harmless pranks.

Fourth, cyber civil rights advocates must overcome the free speech argument asserted by online abusers. Perpetrators of cyber civil rights abuses commonly hide behind powerful free speech norms that both online and offline communities revere. Just as the subjugation of African Americans was justified under the rubrics of states' rights and freedom of contract, destructive online mobs invoke free speech values even as they work to suppress the speech of women and people of color.³¹

Fifth, a cyber civil rights agenda must be sure to highlight the harms inflicted on traditionally subjugated groups, because online civil rights abuses typically affect members of these traditionally subjugated groups disproportionately, but not universally. This makes the problem less conspicuous and easier to dismiss, much as the fact that the existence of *some* people of color and women work and learn in a given workplace or school may give the erroneous impression that hiring or admissions procedures do not impose disproportionate burdens on members of those groups.

Finally, applying civil rights norms to the technological advances of the Information Age requires overcoming the same challenges that law faces in coping with any sweeping social change: inevitable false starts threaten to discredit all legal intervention, giving credibility to arguments that law must ignore harms resulting from new technologies to avoid bringing progress to a grinding halt.³²

This Article analyzes the problem of anonymous online mobs that target women, people of color, and other vulnerable groups and proposes a legal response. In so doing, it seeks to begin a conversation about developing a cyber civil rights agenda more generally.

This Article proceeds in four parts. Part I describes these mobs' behavior and their success in terrorizing victims and suppressing their targets' speech. It also finds that the online environment offers all the same conditions that social psychology research has found to maximize the danger of destructive mob behavior.

³⁰ PHILIP DRAY, *CAPITOL MEN: THE EPIC STORY OF RECONSTRUCTION THROUGH THE LIVES OF THE FIRST BLACK CONGRESSMEN* 99 (2008).

³¹ More generally, opponents of cyber civil rights raise the supposed perils of even modest governmental regulatory involvement with the Internet against initiatives to address any cyber civil rights concerns.

³² See FRIEDMAN, *supra* note 3, at 351 (explaining the U.S. rejection of strict liability as partly attributable to the pressing need to encourage material development).

Part II lays out the necessary components of a legal response to online mobs. First, cyber civil rights proponents should seek to align the interests of dominant online groups with those of online mobs' victims. Second, such proponents must make an effort to translate longstanding civil rights principles from the offline to the online world.

Part III considers the relationship between cyber civil rights and cyber civil liberties. In particular, it addresses both theoretical and doctrinal concerns about limiting online mobs' attacks, which purport to be protected speech. It shows that, although much obnoxious online activity is and should be protected, limiting online mobs' ability to silence women, people of color, and their other targets will, in fact, enhance the most important values underlying the First Amendment.

Finally, Part IV addresses the problems posed by online mobs' anonymity. Whatever causes of action their victims may possess do little good if they cannot find and serve their assailants. Online mobs' ability to strike with impunity results in large part from websites' practices of opening themselves to anonymous posters. Unfortunately, after a misguided, overzealous early case imposed unsustainable strict liability on Internet Service Providers ("ISPs") for material accessed through their facilities, the legal debate has veered unproductively into the language of immunity. This Part instead seeks to move the debate to the development of a standard of care that preserves the benefits from the Internet's aggregative and disaggregative functions while limiting the opportunities for online mobs and others to harness those awesome capabilities for malicious and unlawful ends.

I. ANONYMOUS MOBS OF THE TWENTY-FIRST CENTURY

The most valuable, indeed generative, opportunity the Internet provides is access.³³ An individual must establish an online presence and begin to build an online reputation before aggregating ideas or economic opportunities with others online. The Internet offers no viable alternatives to connect with others if a person is forced off the Internet as compared to the offline world, which offers various means of communication even if one route is foreclosed. And it is through access to the online community that anonymous groups come together to deny women, people of color, religious minorities, lesbians, and gays access.

The civil rights implications of ISPs charging women or African Americans higher monthly fees than men or Caucasians would be obvious. A less obvious, although no less troubling, civil rights problem arises when anonymous online groups raise the price vulnerable people have to pay to maintain an online presence by forcing them to suffer a destructive combination of threats, damaging statements aimed to interfere with their employment opportunities, privacy invasions, and denial-of-service attacks

³³ See JONATHAN ZITTRAIN, *THE FUTURE OF THE INTERNET – AND HOW TO STOP IT* 79-81 (2008).

because of their gender or race. Their assaults force vulnerable people offline, preventing them from enjoying the economic and social opportunities that social networking sites, blogs, and other Web 2.0 platforms provide.

Section A describes these cyber assaults that imperil, economically harm, and silence traditionally disadvantaged people. Section B shows how the online environment magnifies the pathologies driving dangerous group behavior, ensuring that the abuse will not correct itself.

A. *The Destructive Nature of Online Mobs*

Online assaults exist along several, interconnected dimensions.³⁴ First, attacks involve threats of physical violence. Death and rape threats are legion on the web.³⁵ The threats may foreshadow offline stalking and physical violence.³⁶ They often include references to victims' home addresses and personal information, suggesting attackers' familiarity with them, and the attackers encourage readers to physically assault the victims, putting them in fear of genuine danger. Posters also encourage readers to physically assault victims, providing the victims' home address.

In response, victims stop blogging and participating in online forums.³⁷ A Pew Internet and American Life Project study attributed a nine percent decline

³⁴ A note on methodology is in order. Discussing material of this kind in an academic forum raises difficult ethical questions. Repeating damaging material for the sake of condemning it would be counter-productive and, indeed, hypocritical. At the same time, the sheer brutality of these assaults is an important part of this story. This Article repeats the mobs' misogynistic and other bigoted rhetoric to the extent necessary to convey the depth of their depravity, but beyond that paraphrases. It excludes the names of all victims that have not gone fully public themselves.

³⁵ See, e.g., Cheryl Lindsey Seelhoff, *A Chilling Effect: The Oppression and Silencing of Women Journalists and Bloggers Worldwide*, OFF OUR BACKS, Summer 2007, at 18, 18 (describing posters' threats to kill and rape a female writer on her blog); Valenti, *supra* note 5 (describing anonymous posters' attack of women bloggers with comments such as "I would f[**]k them both in the ass" and "hate-f[**]k" them); Posting of Zephoria to Apophenia, *supra* note 13 (providing an account of rape threats on a college computer science message board).

³⁶ Catherine Holahan, *The Dark Side of Web Anonymity*, BUS. WK., May 12, 2008, at 64, 64 *available at* http://www.businessweek.com/magazine/content/08_19/b4083064456431.htm (detailing how a young woman had strange men showing up at her home in response to sexual comments made about her online).

³⁷ Barak, *supra* note 6, at 80; *Female Bloggers Face Harassment*, WOMEN IN HIGHER EDUC., June 1, 2007, at 5, 5 (highlighting that female bloggers are likely to be harassed far more than their male counterparts and that such harassment may have led to a decrease in female presence in online chat rooms); see Nakashima, *supra* note 9 (explaining that women attacked online by anonymous posters respond by suspending blogging, turning to private forums, or using gender-neutral pseudonyms); Elaine Vigneault: Read My Mind, <http://www.elainevigneault.com/> (Apr. 13, 2007) (on file with author) [hereinafter

in women's use of chat rooms to menacing sexual comments.³⁸ Victims may also make their sites private or assume pseudonyms to mask their identity.³⁹ As one victim explains, it does not take many rape threats to "make women want to lay low."⁴⁰

Second, assaults invade victims' privacy. Attackers hack into victims' computers and e-mail accounts to obtain personal information, such as Social Security numbers, driver's license information, and confidential medical data.⁴¹ The stolen information is then posted online.⁴² Disclosing such personal information poses imminent risks, such as the threat of identity theft, employment discrimination, and online or offline stalking.⁴³ It also inflicts harm in the longer term. Victims feel a sustained loss of personal security and regularly dismantle their online presence to avoid further devastation of their privacy.⁴⁴

Third, assaults can involve statements that damage reputations and interfere with victims' economic opportunities.⁴⁵ Online comments may assert that individuals suffer from mental illnesses.⁴⁶ They may claim individuals have sexually transmitted diseases.⁴⁷ Attackers sometimes publish doctored photographs of victims.⁴⁸ In addition, attackers send damaging statements about victims to their employers and manipulate search engines to reproduce

Vigneault, *Ignore Violence*] (explaining that she assumes male pseudonyms to comment on male-dominated blogs).

³⁸ *Female Bloggers Face Harassment*, *supra* note 37, at 5.

³⁹ *Id.*

⁴⁰ Valenti, *supra* note 5.

⁴¹ Barak, *supra* note 6, at 80.

⁴² See Pat Miller, *Another Rape in Cyberspace*, CERISE, Nov. 2007, <http://cerise.theirisnetwork.org/archives/188>.

⁴³ See Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 252-53 (2007) (discussing the risk of identity theft posed by the release of Social Security numbers).

⁴⁴ Nakashima, *supra* note 9.

⁴⁵ Victims maintain that many of these statements are false. If indeed that is true, such postings may be tortious. See *infra* Part III.C.1. (discussing defamation and false light claims). This Article will not attempt to parse the truth of particular charges.

⁴⁶ See, e.g., Sandra Sobieraj Westfall et al., *Campus Controversy: Has Online Gossip Gone Too Far?*, PEOPLE, Apr. 14, 2008, at 107 (explaining that anonymous posters on the JuicyCampus website asserted that a Duke student attempted suicide, which the student claimed was false).

⁴⁷ See Richard Morgan, *A Crash Course in Online Gossip*, N.Y. TIMES, Mar. 16, 2008, at ST7; Jessica Bennett, *The Flip Side of Internet Fame*, NEWSWEEK, Feb. 22, 2008, <http://www.newsweek.com/id/114535> (describing JuicyCampus as having turned into a venue for bigoted rants and stories about identified students' alleged drug use and sexual diseases).

⁴⁸ See Valenti, *supra* note 5.

the damaging statements and pictures for others to see,⁴⁹ creating digital “scarlet letters” that destroy reputations.⁵⁰

Fourth, some assaults do not involve online postings at all. Instead, attackers use technology to force victims offline. Groups coordinate denial-of-service attacks⁵¹ and “image reaping” campaigns to shut down sites and blogs.⁵² While the other types of assaults silence victims indirectly with fear and humiliation, this fourth type of assault muzzles them directly.

Groups commonly wield all four of these tools in their attacks against individuals. Some attacks originate online and continue offline, while others move in the opposite direction.⁵³ For example, in 2007, the social networking site AutoAdmit hosted a pattern of attacks on female law students.⁵⁴ Thirty-

⁴⁹ See SOLOVE, *supra* note 4, at 203 (explaining that employers conduct background checks by running Google searches which often produce inaccurate information).

⁵⁰ Frank Pasquale, *Rankings, Reductionism, and Responsibility*, 54 CLEV. ST. L. REV. 115, 122 (2006); Adam Hunter, *Click Here for Justice?*, <http://tech.msn.com/news/article.aspx?cp-documentid=6247087> (last visited Nov. 2, 2008) (“The Puritans had their scarlet letters to shame those accused of wrongdoing; today, we have the Internet.”).

⁵¹ Greer, *supra* note 8; Elaine Vigneault: Read My Mind, <http://www.elainevigneault.com/> (Aug. 11, 2007) (on file with author) [hereinafter Vigneault, *Web Harassment*]. A denial-of-service attack is conduct that causes a loss in service of online resources. A common form of denial-of-service is a buffer overflow attack in which attackers send multiple e-mails, requests for information, or other traffic to the server or network address to shut it down. Catherine E. Smith, *Intentional Infliction of Emotional Distress: An Old Arrow Targets the New Head of the Hate Hydra*, 80 DENV. U. L. REV. 1, 4 n.23 (2002). In November 2001, the FBI reported that extremist groups were adopting the power of modern technology and concluded that, although extremist groups’ cyberattacks were limited to unsophisticated e-mail bombs and threatening content, the increase in technological competency could lead to network-based attacks on the nation’s infrastructure such as shutting down government computer systems. See NAT’L INFRASTRUCTURE PROT. CTR., HIGHLIGHTS 2-4 (Linda Garrison & Martin Grand eds., 2001), <http://www.iwar.org.uk/infocon/nipc-highlights/2001/highlight-01-10.pdf>; Brian McWilliams, *Internet an Ideal Tool for Extremists - FBI*, NEWSBYTES, Nov. 16, 2001, available at 2001 WLNR 6085044.

⁵² “Image reaping” involves the repeated refreshing of a site’s images to use up all of its allocated bandwidth. Vigneault, *Web Harassment*, *supra* note 51.

⁵³ See, e.g., Posting of AmandaBrumfield to BlogHer, <http://www.blogher.com/node/12104> (Mar. 30, 2007, 11:16) (explaining that she shut down her personal blog after a year of being stalked and harassed by a group of people both online and offline including calls to her father’s unlisted phone number with threats).

⁵⁴ Brittan Heller, Note, *Of Legal Rights and Moral Wrongs: A Case Study of Internet Defamation*, 19 YALE J.L. & FEMINISM 279, 285 n.20 (2007) (explaining that targeted female law students attended various law schools including Boston University, Harvard, New York University, Northwestern, University of Virginia, and Yale).

nine posters targeted named students on the site's message board.⁵⁵ The posters, writing under pseudonyms, generated hundreds of threatening, sexually-explicit, and allegedly defamatory comments about the victims.⁵⁶

Posters threatened female law students with violence. One poster asserted that a named female student should "be raped."⁵⁷ That remark begat dozens of more threats. For instance, a poster promised: "I'll force myself on [the identified student]" and "sodomize" her "repeatedly."⁵⁸ Another said the student "deserves to be raped so that her little fantasy world can be shattered by real life."⁵⁹

Discussion threads suggested the posters had physical access to the female students. A poster described a student's recent attire at the law school gym.⁶⁰ Posts mentioned meeting targeted women and described what they looked like and where they spent their summer.⁶¹ Posters urged site members to follow a woman to the gym, take her picture, and post it on AutoAdmit.⁶² Others provided updates on sightings of a particular woman.⁶³ Another poster

⁵⁵ Posting of Amir Efrati to Wall Street Journal Law Blog, <http://blogs.wsj.com/law/2008/01/30/subpoena-allowed-in-autoadmit-suit> (Jan. 30, 2008, 9:08 EST).

⁵⁶ Plaintiffs' Memorandum of Law in Support of Opposition to John Doe 21's Motion to Quash Plaintiff's Subpoena at 6, *Doe I v. Individuals*, 561 F. Supp. 2d 249 (D. Conn. 2008) (No. 3:07CV00909) [hereinafter Plaintiffs' Memorandum of Law] (explaining that AutoAdmit members posted over 200 threads about named female law students).

⁵⁷ First Amended Complaint ¶ 49, *Doe I*, 561 F. Supp. 2d 249 (No. 307CV00909) [hereinafter First Amended Complaint]; Letter from John Doe 21, a.k.a. "AK47" to Plaintiffs, *reprinted in* Declaration of Steve Mitra in Support of Plaintiffs' Opposition to John Doe 21's Motion to Quash Plaintiffs' Subpoena exhibit 4, at 2, *Doe I*, 561 F. Supp. 2d 249 (No. 307CV00909) (admitting that the author posted a comment that plaintiff "should be raped").

⁵⁸ First Amended Complaint, *supra* note 57, ¶ 21.

⁵⁹ *Id.* ¶ 23. Similarly, two female bloggers received e-mails from anonymous individuals threatening sexual violence and faced in-person harassment after resigning from John Edwards' presidential campaign in 2007. Posting of Amanda Marcotte to Pandagon, <http://pandagon.blogsome.com/2007/02/13/people-who-claim-to-love-jesus-write-me/> (Feb. 13, 2007); Posting of Paul the Spud to Shakesville, <http://www.shakespearessister.blogspot.com/2007/03/this-needs-to-stop.html> (Mar. 27, 2007) (describing individuals "blocking [a female blogger's] driveway and pounding on her door").

⁶⁰ Plaintiff's Memorandum of Law, *supra* note 56, at 4.

⁶¹ Jill Filipovic, Note, *Blogging While Female: How Internet Misogyny Parallels "Real-World" Harassment*, 19 YALE J.L. & FEMINISM 295, 295 (2007).

⁶² Plaintiff's Memorandum of Law, *supra* note 56, at 4.

⁶³ Filipovic, *supra* note 61, at 296 (explaining that AutoAdmit posters described sightings of the author alongside comments that she should be "hate f[**]k[ed]" and "kick[ed in] the box").

provided the e-mail address of a female law student under a thread entitled “Mad at [named individual]? E-mail her”⁶⁴

Posters also asserted damaging statements about the women. One asserted that a female student spent time in a drug rehabilitation center.⁶⁵ Another claimed the student had a lesbian affair with a law school administrator.⁶⁶ Others remarked that the student appeared in *Playboy*.⁶⁷ Posters claimed that another female student had a sexually transmitted disease.⁶⁸ Others provided her purported “sub-par” LSAT score.⁶⁹ The victims asserted that these were lies.⁷⁰

In addition to publishing the alleged lies online, posters spread them offline to undermine the victims’ job opportunities. One poster urged the group to tell top law firms about the female student’s LSAT score “before she gets an offer.”⁷¹ Posters e-mailed their attacks to the student’s former employer, recommending that the employer show it to its clients, who would “not want to be represented by someone who is not of the highest character value.”⁷²

Another poster sent an e-mail to a particular female law student’s faculty asserting that her father had a criminal record.⁷³ The poster displayed the e-mail on AutoAdmit before sending it, explaining: “I’ve assembled a spreadsheet with [the faculty e-mail] addresses and every single one of them will be notified about what our darling [named student] has done. I post this here as a warning to all those who would try to regulate the more antisocial posters – we have the power now.”⁷⁴

⁶⁴ First Amended Complaint, *supra* note 57, ¶ 63.

⁶⁵ *Id.* ¶ 54. Similarly, two female bloggers received e-mails from anonymous individuals threatening sexual violence and faced in-person harassment after resigning from John Edwards’ presidential campaign in 2007. Posting of Amanda Marcotte to Pandagon, <http://pandagon.blogspot.com/2007/02/13/people-who-claim-to-love-jesus-write-me/> (Feb. 13, 2007); Posting of Paul the Spud to Shakesville, <http://www.shakespearessister.blogspot.com/2007/03/this-needs-to-stop.html> (Mar. 27, 2007) (describing individuals “blocking [a female blogger’s] driveway and pounding on her door”).

⁶⁶ *Id.* ¶ 27.

⁶⁷ *Id.* ¶ 51.

⁶⁸ *Id.* ¶ 21.

⁶⁹ *Id.* ¶¶ 26, 28, 30.

⁷⁰ *Id.* ¶¶ 32, 52-54, 79-82. Whether the assertions are indeed false statements is raised by the plaintiffs’ lawsuit against the thirty-nine AutoAdmit posters. See Heller, *supra* note 54, at 280 (explaining that the “ludicrous allegations” made against one of the victims included false accusations that she “bribed [her] way into Yale with an ‘embarrassingly low amount’ of money” and “pretend[ed] to be either African-American or Native-American”).

⁷¹ First Amended Complaint, *supra* note 57, ¶ 30.

⁷² *Id.* ¶ 61.

⁷³ *Id.* ¶ 58.

⁷⁴ *Id.* ¶ 59.

Site members applauded the e-mail and rallied around the sender. For instance, a poster stated that the e-mail sender should be awarded a “Congressional medal.”⁷⁵ Others recommended sending the e-mail from a public PC and a “hushmail account” or with anonymizing software.⁷⁶

The attackers waged a “Google-bombing” campaign that would ensure the prominence of offensive threads in searches of the female students’ names.⁷⁷ Posters made plain the goal of their Google-bombing campaign: “We’re not going to let that bitch have her own blog be the first result from googling her name!”⁷⁸ An individual writing under the pseudonym “leaf” detailed the steps AutoAdmit posters would have to take to engage in Google-bombing.⁷⁹ Leaf explained that posts should include the adjective “big-titted” next to the woman’s name.⁸⁰ “Big-titted [name of female student]’s name is never to be used in parts – it must always be [name of student] at the least, and ‘big-titted [name of the student]’ ideally” with pictures of her accompanying the thread.⁸¹ This would work because search engine algorithms assign a high rank to a web page if sites linking to that page use consistent anchor text.⁸²

Posters admitted their desire to intimidate and harm the female students. After one of the women did not get a summer job, a poster asked if the other “bitch got what she deserved too?”⁸³ Another said: “I’m doing cartwheels

⁷⁵ Posting of Bodhi Tree Miracle to AutoAdmit, <http://www.autoadmit.com/> (Mar. 9, 2007, 14:34) (on file with author).

⁷⁶ Posting of atlas (flae) to AutoAdmit, <http://www.autoadmit.com/> (Mar. 9, 2007, 15:45) (on file with author).

⁷⁷ See First Amended Complaint, *supra* note 57, ¶ 17.

⁷⁸ Posting of STANFORDtroll to AutoAdmit, <http://www.autoadmit.com/> (Mar. 9, 2007, 12:39) (on file with author).

⁷⁹ First Amended Complaint, *supra* note 57, ¶ 43.

⁸⁰ *Id.*

⁸¹ *Id.*

⁸² See Tom McNichol, *Your Message Here*, N.Y. TIMES, Jan. 22, 2004, at G1; Tom Zeller, Jr., *A New Campaign Tactic: Manipulating Google Data*, N.Y. TIMES, Oct. 26, 2006, at A20. Previously, Google asserted it has little or no control over the practice of Google-bombing and would not individually edit search results due to the fact that a bomb occurred. Posting of Marissa Mayer, Director of Consumer Web Products to The Official Google Blog, <http://googleblog.blogspot.com/2005/09/googlebombing-failure.html> (Sept. 16, 2005, 12:54). On January 27, 2007, Google announced on its official Google Webmaster Central Blog that it now had an “algorithm that minimizes the impact of many Googlebombs.” Posting of Ryan Moulton & Kendra Carattini to The Official Google Webmaster Central Blog, <http://googlewebmastercentral.blogspot.com/2007/01/quick-word-about-googlebombs.html> (Jan. 25, 2007, 16:16).

⁸³ Posting of STANFORDtroll to AutoAdmit, <http://www.autoadmit.com/> (Mar. 9, 2007, 12:42) (on file with author).

knowing this stupid Jew bitch is getting her self esteem raped.”⁸⁴ A poster explained that the women were targeted “just for being women.”⁸⁵

A lawsuit filed by two of the women alleged the AutoAdmit site managers refused to remove the offensive threads even though the women told them that the messages caused them severe emotional distress.⁸⁶ On March 15, 2007, a site manager asserted that he would not remove the offensive threads until the female students apologized for threatening litigation and until ReputationDefender, a group assisting the women, acknowledged the mistakes the manager alleged the group had made.⁸⁷

In a similar vein, a group called Anonymous has devoted itself to terrorizing and silencing hundreds of women writing on the Web.⁸⁸ For instance, in 2007, Anonymous used message boards and wikis to plan an attack on a nineteen-year-old woman who maintained a video blog about Japanese language and video games.⁸⁹ Group members hacked her online accounts, including her YouTube blog account, e-mail, Facebook profile, and MySpace page, to obtain

⁸⁴ First Amended Complaint, *supra* note 57, ¶ 42.

⁸⁵ Posting of roffles roffles to AutoAdmit, <http://www.autoadmit.com/> (Mar. 11, 2007, 21:50) (on file with author).

⁸⁶ First Amended Complaint, *supra* note 57, ¶ 15. The former Chief Education Director of AutoAdmit filed a libel suit against two female law students, their counsel, and ReputationDefender, in which he disputed the students’ claim that he refused their requests to take down the offensive threads. Complaint ¶¶ 30, 33, *Ciolti v. Iravani*, No. 2:08CV02601, 2008 WL 4412053 (E.D. Pa. 2008) (alleging that “Mr. Ciolti never told [defendant] that any postings about her would not be removed” and that he responded to a complaint sent by the defendant with a message that she should direct her concerns to site owner Jarret Cohen).

⁸⁷ Jarret Cohen, AutoAdmit’s Challenge to Reputation Defender (Mar. 15, 2007), <http://www.autoadmit.com/challenge.to.reputation.defender.html>. Cohen said that one of the identified women contacted him to remove offensive messages about her, but he ignored her request because she threatened to sue him. Mary E. O’Leary, *Open Website Hurts: Yale Group Stands up Against Offensive Content*, NEW HAVEN REG., Apr. 1, 2007. Cohen also asserted that he dismissed another similar complaint “because it sounded like more of the kind of juvenile stuff that I have heard going on that people complained about for years.” *Id.* (quoting Jarret Cohen).

⁸⁸ Unidentified individuals began Anonymous in 2003. The group has gathered its members on online image boards, such as 4chan.org. Chris Landers, *Serious Business: Anonymous Takes on Scientology*, CITY PAPER (Balt.), Apr. 2, 2008, at 14. As of April 2008, 4chan.org is the fifty-sixth most popular website in the United States. *Id.* A 2006 news special on Fox’s Los Angeles affiliate gave Anonymous some notoriety by featuring the group in a story, which described the group as “hackers on steroids” and an “internet hate machine.” *Id.*; see *FOX 11 Investigates: ‘Anonymous’* (FOX 11 news broadcast July 26, 2007), <http://www.youtube.com/watch?v=DNO6G4ApJQY>.

⁸⁹ Miller, *supra* note 42. The woman maintained her video blog under the name Applemilk1988. *Id.* Before the attacks, the woman’s blog garnered broad attention, making it onto YouTube’s Most Subscribed list. *Id.* A wiki is a webpage designed so that any user may modify or add to its content.

her personal information.⁹⁰ They published her account passwords and private medical history on various sites.⁹¹ Postings disclosed her full name, home address, and her mother's e-mail address.⁹² Group members sent messages from the woman's e-mail account to her loved ones.⁹³ They claimed the woman had committed suicide on various message boards.⁹⁴

Members of Anonymous posted doctored photographs of the woman including one picture that featured the woman's head atop naked bodies.⁹⁵ Next to her picture appeared the promise that group members would rape her "at full force in her vagina, mouth, and ass."⁹⁶ A drawing depicted men brutally raping the woman.⁹⁷

Anonymous urged its members to "seek and destroy" the woman's online identity.⁹⁸ Group members saturated her video blog with sexually violent material.⁹⁹ They took down her videos.¹⁰⁰ Anonymous updated its members on the status of her sites.¹⁰¹ When her live journal or video blog reappeared, Anonymous urged members to "rape" and "nuke[] [her sites] from orbit."¹⁰²

Anonymous similarly attacked a journalist writing under the pseudonym "Heart" who maintained a blog and discussion forum about women's issues.¹⁰³ Group members pieced together her identity from her postings and revealed her name and home address on her discussion forum.¹⁰⁴ They made death threats and sexually menacing comments on her blog.¹⁰⁵ Anonymous urged

⁹⁰ *Id.*; see Encyclopedia Dramatica, Applemilk1988, <http://www.encycopediadramatica.com/Applemilk1988> (last visited Nov. 2, 2008) [hereinafter Applemilk1988].

⁹¹ Applemilk1988, *supra* note 90; Miller, *supra* note 42.

⁹² See Applemilk1988, *supra* note 90; Insurgency Wiki, Applemilk, <http://partyvan.info/index.php?title=Applemilk> (last visited Nov. 2, 2008).

⁹³ Miller, *supra* note 42.

⁹⁴ *Id.*

⁹⁵ *Id.*

⁹⁶ *Id.*

⁹⁷ *Id.*

⁹⁸ Applemilk1988, *supra* note 90.

⁹⁹ Miller, *supra* note 42.

¹⁰⁰ Applemilk1988, *supra* note 90.

¹⁰¹ *Id.*

¹⁰² *Id.*

¹⁰³ Posting of Heart to Women's Space, <http://womensspace.wordpress.com/2007/08/06/blogging-while-female-men-win-hacking-as-sexual-terrorism/> (Aug. 6, 2007) [hereinafter Heart].

¹⁰⁴ Greer, *supra* note 8.

¹⁰⁵ A poster wrote: "I'd like to tie you down, take a knife, and slit your throat. I'd penetrate you over and over in all orifices, and create some of my own to stick myself in." Posting of Heart to Women's Space, *Bloggng While Female – Warning May Trigger*, <http://womensspace.wordpress.com/2007/08/04/blogging-while-female-warning-may-trigger/> (Aug. 4, 2007).

members to engage in “image reaping” to shut down her site.¹⁰⁶ The group succeeded in overloading and closing Heart’s website during the summer of 2007.¹⁰⁷ In August 2007, Heart closed her blog and website.¹⁰⁸

Anonymous maintains a list of sites and blogs addressing women’s issues that it claims to have forced offline.¹⁰⁹ The list includes the names of shuttered sites with a line crossed through them and the accompanying message: “Down due to excessive bandwidth – great success!”¹¹⁰ When a site reappears online, Anonymous tells its members: “It’s back! Show no mercy.”¹¹¹ The group takes credit for closing over 100 feminist sites and blogs.¹¹² Anonymous has also targeted journalists, such as Anna Greer, who have reported on the group’s attacks. The group published Ms. Greer’s home and e-mail addresses with instructions to “choke a bitch.”¹¹³

Targeted female bloggers and website operators confirm the group’s claims of attacks.¹¹⁴ They describe the denial-of-service attacks and “image reaping” campaigns that have shut down their sites.¹¹⁵ A victim explained: “Being silenced for over two weeks felt infuriating, stifling, imprisoned by gang raepists [sic] just waiting for me to try to get up from underneath their weight

¹⁰⁶ Heart, *supra* note 103.

¹⁰⁷ *Id.* ISPs provide the websites they host with monthly bandwidth allocations. When a site uses up its monthly allowance, the ISP will shut down the site until the following month or charge the website owner additional fees. ISPs have a variety of hosting plans and usually charge monthly rates. See, e.g., HostDime, Shared Website Hosting Services and Plans, <http://www.hostdime.com/services/shared/> (last visited Nov. 25, 2008).

¹⁰⁸ Heart, *supra* note 103.

¹⁰⁹ See Encyclopedia Dramatica, Cheryl Lindsey Seelhoff, http://www.encyclopedia-dramatica.com/Cheryl_Lindsey_Seelhoff (last visited Nov. 2, 2008) [hereinafter Seelhoff].

¹¹⁰ Seelhoff, *supra* note 109.

¹¹¹ *Id.*

¹¹² Posting of Jill to Feministe, <http://www.feministe.us/blog/archives/2007/08/09/what-do-we-do-about-online-harassment/> (Aug. 9, 2007, 22:36).

¹¹³ Insurgency Wiki, Anna Greer, http://partyvan.info/index.php?title=Anna_Greer (last visited Nov. 3, 2008).

¹¹⁴ Posting of Kevin to A Slant Truth, <http://slanttruth.com/2007/08/15/feminist-bloggers-are-under-increasing-levels-of-attack/> (Aug. 15, 2007, 20:15 EST) (explaining that feminist blogs including Feministe, Shakesville, Women’s Space, and Biting Beaver were subjected to denial-of-service attacks). For instance, freesoil.org was shut down due to excess bandwidth. Posting of Aletha to Women’s Space, <http://womensspace.wordpress.com/2007/08/06/bloggng-while-female-men-win-hacking-as-sexual-terrorism/#comment-47470> (Aug. 7, 2007, 7:20 EST). Freesoil.org’s web access log showed evidence of a denial-of-service attack. Posting of Aletha to Free Soil Party Blog, <http://freesoil.org/wordpress/?p=221> (Sept. 18, 2007, 1:41 EST) [hereinafter Aletha – Free Soil Party Blog]. In addition, “Newwaveradfem” explained that her blog was attacked in August 2007. New Wave Radical Blog, <http://newwaveradfem.wordpress.com/?s=attack> (Aug. 4, 2007, 14:40).

¹¹⁵ Vigneault, *Ignore Violence*, *supra* note 37.

so they could stomp me down again.”¹¹⁶ Victimized website operators and bloggers have asked the group Anonymous in vain to stop its attacks.¹¹⁷

Groups attack women on the website JuicyCampus with threats of violence, and their posts have generated offline stalking.¹¹⁸ For instance, anonymous posters disclosed a woman’s cell phone and dorm address with instructions that she was available for sex.¹¹⁹ After the posts appeared, strange men started knocking on the woman’s door at night.¹²⁰

Online mobs have targeted African-American and Hispanic women.¹²¹ As blogger “La Chola” explains, women-of-color bloggers have consistently received horrific, vile e-mails and comments threatening violent sexual assault, death, and attacks against family members.¹²² After the author of the blog “Ask This Black Woman” posted commentary about the Resident Evil 5 video game, anonymous posters attacked her on her blog and other sites.¹²³ She received death threats.¹²⁴ Posters told her to “[g]et back into the cotton fields, you filthy [n***r]”¹²⁵ and threatened to overrun her blog.¹²⁶

Posters on a white supremacist website targeted Bonnie Jouhari, the mother of a biracial girl.¹²⁷ The site posted an image of Jouhari’s workplace burning in flames with a caption that read “race traitor . . . beware, for in our day, they will be hung from the neck from the nearest tree or lamp post.”¹²⁸ The site included a picture of Jouhari’s child and an image of her burning office with bomb-making instructions posted beneath it.¹²⁹ Ms. Jouhari and her daughter received harassing phone calls at home and at work.¹³⁰

¹¹⁶ Aletha - Free Soil Party Blog, *supra* note 114.

¹¹⁷ *See, e.g., id.*

¹¹⁸ Larry Magid, Opinion, *JuicyCampus is a Haven for Cyberbullies*, SAN JOSE MERCURY NEWS, Mar. 24, 2008, https://www.reputationdefender.com/viewPress?press_id=253.

¹¹⁹ Holahan, *supra* note 36, at 64; Magid, *supra* note 118.

¹²⁰ Holahan, *supra* note 36, at 64.

¹²¹ Posting of La Chola to La Alma de Fuego, <http://brownfemipower.com/?p=1224> (Apr. 13, 2007, 11:15).

¹²² *Id.*

¹²³ Posting of Sokari to Black Looks, http://www.blacklooks.org/2007/08/where_lies_the_resident_evil.html (Aug. 1, 2007).

¹²⁴ Ask This Black Woman, <http://askthisblackwoman.com/2007/10/01/death-threat.aspx> (Oct. 1, 2007, 15:20).

¹²⁵ Ask This Black Woman, <http://askthisblackwoman.com/2007/08/01/more-on-resident-evil-5.aspx> (Aug. 1, 2007, 11:52).

¹²⁶ Vigneault, *Ignore Violence*, *supra* note 37.

¹²⁷ Wilson, No. 03-98-0692-8, 2000 WL 988268, at *4 (Dep’t of Hous. & Urban Dev. July 19, 2000).

¹²⁸ *Id.*

¹²⁹ *Id.* at *4, *6.

¹³⁰ *Id.* at *7.

Other people of color have faced similar attacks.¹³¹ An Asian-American columnist who writes a blog called “Yellow Peril” explained that a group of individuals attacked her online after she wrote about a hate crimes march.¹³² The group posted a picture of her on a white supremacist watch list, which included her phone number and address, and its members sent threatening e-mails to her.¹³³ College students wrote racially threatening messages on a Hispanic student’s Facebook profile,¹³⁴ promising to “come find you and drag you behind my (expletive) car.”¹³⁵

Online mobs target individuals from religious minorities as well. Groups post anti-Semitic comments alongside damaging statements about specific Jewish individuals on the website JuicyCampus.¹³⁶ The group Anonymous has targeted the Church of Scientology.¹³⁷ It posted videos on YouTube announcing its intent to destroy the Church.¹³⁸ Anonymous calls its campaign

¹³¹ See, e.g., MinJungKim.com Braindump v. 6.0, <http://minjungkim.com/2007/03/26/it%e2%80%99s-awful-yes/> (Mar. 26, 2007, 17:00 EST) (describing one Asian-American woman’s experience with threatening e-mails, racist online comments, and instant message harassment).

¹³² Washington Baltimore and Annapolis Blog, <http://www.crablaw.com/2007/04/take-back-blog-host-page.html>.

¹³³ *Id.* Similarly, a woman who maintained a blog about Persian culture reported that her site was hacked and that individuals posted pornographic pictures and her home address on the site. Posting of Lady Sun to Women’s Space, <http://womensspace.wordpress.com/2007/08/06/blogging-while-female-men-win-hacking-as-sexual-terrorism/#comment-48188> (Aug. 9, 2007, 5:05).

¹³⁴ Christine Reid, *Lawyer: O’Neal Not Responsible*, BOULDER DAILY CAMERA, Feb. 28, 2006, at A1.

¹³⁵ Vincent Carroll, Editorial, *On Point: Blurring the Line*, ROCKY MTN. NEWS, June 6, 2006, at 34A. In 1996, Richard Machado, a former student at the University of California at Irvine, sent anonymous messages signed “Asian Hater” to fifty-nine Asian students. ComputingCases.org, Machado Case History, http://computingcases.org/case_materials/machado/case_history/case_history.html (last visited Nov. 4, 2008). In the message, the student warned that he would “personally . . . find and kill” his target. *Id.* Machado was convicted of two counts of federal civil rights violations. *Id.*

¹³⁶ *California Middle-Schoolers Suspended for Viewing MySpace Posting with Alleged Threat*, SAN DIEGO UNION-TRIB., Mar. 2, 2006, <http://www.signonsandiego.com/news/nation/20060302-1140-myspace-suspensions.html> (reporting that twenty middle school students were suspended for two days after viewing a boy’s posting that contained anti-Semitic remarks and threats against another student).

¹³⁷ See Landers, *supra* note 88 (quoting a statement by Anonymous that it intends to “expel” the Church of Scientology from the Internet and “systematically dismantle” the religious group); Posting by Ryan Singel to Wired Blog Network, <http://blog.wired.com/27bstroke6/2008/01/anonymous-hack.html> (Jan. 25, 2008, 18:39) (describing an attack by Anonymous, intended for a Scientology website, that instead attacked the website of a school in the Netherlands).

¹³⁸ Landers, *supra* note 88.

against the religious organization “Project Chanology.”¹³⁹ Group members have engaged in denial-of-service attacks to take down the scientology.org website.¹⁴⁰ Nine hundred Anonymous members gathered in a chat room to discuss different ways to harass the Church.¹⁴¹ Some suggested making harassing phone calls to the Church’s local branches.¹⁴²

Online groups have attacked gays and lesbians.¹⁴³ Anonymous has declared homosexuals as the group’s enemy.¹⁴⁴ It urges members to shut down blogs and websites of targeted men and women.¹⁴⁵ Anonymous takes credit for driving “Gay Diamond,” a lesbian, off YouTube.¹⁴⁶ Anonymous accuses victims of having sexually transmitted diseases.¹⁴⁷ Postings reveal targeted individuals’ home addresses, phone numbers, and other personal information.¹⁴⁸ In August 2007, denial-of-service attacks shut down a gay-gaming site and the site’s owners received death threats.¹⁴⁹

The harm online mobs inflict is potent. The threats and privacy intrusions produce damage in numerous ways. Publishing a woman’s home address alongside the suggestion that she should be raped or is interested in sex raises the risk that readers of the post will stalk her or commit physical violence against her. Posting a person’s Social Security number increases the chance that she will be subject to identity theft. Victims fear that threats or identity theft will be realized: the Internet’s anonymity disaggregates the threats from their social context, eliminating cues that might signal the extent of peril. Online anonymity also may prevent an effective law enforcement response. A

¹³⁹ *Id.*

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

¹⁴² *Id.*

¹⁴³ *E.g.*, Aletha - Free Soil Party Blog, *supra* note 114.

¹⁴⁴ *See, e.g.*, Encyclopedia Dramatica, Chris Crocker, http://www.encyclopediadramatica.com/Chris_Crocker (last visited Nov. 5, 2008) [hereinafter Chris Crocker] (espousing hate for Chris Crocker, a gay man who gained fame on YouTube for a video he posted which depicted him crying and urging the public to leave Britney Spears alone).

¹⁴⁵ *See* Encyclopedia Dramatica, Mrfetch, <http://encyclopediadramatica.com/index.php?title=Mrfetch&printable=yes> (last visited Nov. 24, 2008) [hereinafter Mrfetch]; Insurgency Wiki, Keith Kurson, http://partyvan.info/index.php?title=Keith_Kurson (last visited Nov. 5, 2008) [hereinafter Keith Kurson].

¹⁴⁶ *See* Mrfetch, *supra* note 145.

¹⁴⁷ *See* Chris Crocker, *supra* note 144.

¹⁴⁸ Keith Kurson, *supra* note 145.

¹⁴⁹ Posting of Brian Crecente to Kotaku, <http://kotaku.com/gaming/crime/gaygamer-target-of-hate-crime-286127.php> (Aug. 5, 2007, 11:32).

victim's feeling that she is "being watched" also may stifle her creativity and sense of well-being.¹⁵⁰

Victims may lose job opportunities due to damaging statements and threats posted online. Employers often review Google search results before interviewing and hiring candidates.¹⁵¹ The damaging statements and threats may raise doubts about the victim's competence, or suggest the victim attracts unwanted controversy, causing the employer to hire someone else. When victims stop blogging because of threats, they lose opportunities to establish their online presence in a manner that could enhance their careers and attract clients.¹⁵²

If online groups select victims for abuse based on their race, ethnicity, gender, or religion, they perpetrate invidious discrimination. Important parallels exist between the harm inflicted by prior centuries' mobs and this century's destructive online crowds. Much like their offline counterparts, online hate mobs deprive vulnerable individuals of their equal right to participate in economic, political, and social life. They silence victims and stifle public discourse.¹⁵³ Although online mobs do not engage in lynching and physical beatings, their attacks produce serious individual and societal harm that cannot be ignored.

B. *The Dynamics of Mob Behavior*

These destructive crowds continue a disturbing pattern from the past, when anonymous groups such as the anti-immigrant mobs of the nineteenth century and the Ku Klux Klan inflicted serious harm on their victims.¹⁵⁴ Social scientists have identified four factors that influence the potential dangerousness of a group.¹⁵⁵

First, groups with homogeneous views tend to become more extreme when they deliberate.¹⁵⁶ Group members' interactions tend to reinforce preexisting views as members offer a disproportionately large number of arguments

¹⁵⁰ See Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000).

¹⁵¹ See Pasquale, *supra* note 50, at 127.

¹⁵² Penelope Trunk's Brazen Careerist, <http://blog.penelopetrunk.com/2007/07/19/blog-under-your-real-name-and-ignore-the-harassment/> (July 19, 2007) (explaining that women who write under pseudonyms miss opportunities associated with blogging under their real names, such as networking opportunities and expertise associated with the author's name).

¹⁵³ See OWEN M. FISS, *THE IRONY OF FREE SPEECH* 15-16 (1996) (discussing the silencing affect of hate speech).

¹⁵⁴ See generally SHERRILYN A. IFILL, *ON THE COURTHOUSE LAWN: CONFRONTING THE LEGACY OF LYNCHING IN THE TWENTY-FIRST CENTURY* (2007) (discussing the history of lynching and mob behavior in America).

¹⁵⁵ See, e.g., J.S. MCCLELLAND, *THE CROWD AND THE MOB: FROM PLATO TO CANETTI* 196-97 (1989).

¹⁵⁶ See ROGER BROWN, *SOCIAL PSYCHOLOGY: THE SECOND EDITION* 200-06, 222 (1986).

supporting their views and only a small number of arguments tilting the other way.¹⁵⁷ Hearing agreement from others bolsters group members' confidence, entrenching and radicalizing their views.¹⁵⁸

Second, a group member's deindividuation encourages the member to act on destructive impulses.¹⁵⁹ According to one school of thought, people in groups fail to see themselves as distinct individuals and lose a sense of personal responsibility for their destructive acts.¹⁶⁰ Another school of thought attributes deindividuation to anonymity rather than an individual's immersion in a group. This account explains that people behave aggressively when they believe that they cannot be observed and caught.¹⁶¹

Third, groups are more destructive when they dehumanize their victims.¹⁶² By viewing victims as devoid of humanity and personal identity, group

¹⁵⁷ CASS R. SUNSTEIN, *REPUBLIC.COM 2.0*, at 64-67 (2007).

¹⁵⁸ See JOHN C. TURNER ET AL., *REDISCOVERING THE SOCIAL GROUP: A SELF-CATEGORIZATION THEORY* 142 (1987).

¹⁵⁹ See Ed Diener, *Deindividuation: The Absence of Self-Awareness and Self-Regulation in Group Members*, in *PSYCHOLOGY OF GROUP INFLUENCE* 209, 218 (Paul B. Paulus ed., 1980).

¹⁶⁰ See GUSTAVE LE BON, *THE CROWD: A STUDY OF THE POPULAR MIND* 26 (1896); Brian Mullen, *Operationalizing the Effect of the Group on the Individual: A Self-Attention Perspective*, 19 *J. EXPERIMENTAL SOC. PSYCHOL.* 295, 295 (1983); Tom Postmes & Russell Spears, *Deindividuation and Antinormative Behavior: A Meta-Analysis*, 123 *PSYCHOL. BULL.* 238, 254 (1998).

¹⁶¹ ARNOLD P. GOLDSTEIN, *THE PSYCHOLOGY OF GROUP AGGRESSION* 32 (2002); RALPH H. TURNER & LEWIS M. KILLIAN, *COLLECTIVE BEHAVIOR* 165, 408 (2d ed. 1972); PHILIP G. ZIMBARDO, *THE LUCIFER EFFECT: UNDERSTANDING HOW GOOD PEOPLE TURN EVIL* 25 (2007). This insight naturally accords with deterrence theory. Studies show heightened aggression in subjects who feel anonymous. The Zimbardo study asked participants to administer electric shocks to their subjects. Philip G. Zimbardo, *The Human Choice: Individuation, Reason, and Order Versus Deindividuation, Impulse, and Chaos*, in *NEBRASKA SYMPOSIUM ON MOTIVATION* 237, 266-70 (W.J. Arnold & David Levin eds., 1969). Some participants wore oversized lab coats and hoods while others wore normal attire. *Id.* at 264. The hooded participants shocked their subjects longer than the identifiable participants did. *Id.* at 268; see also Evan R. Harrington, *The Social Psychology of Hatred*, 3 *J. HATE STUD.* 49, 60-61 (2005) (describing a study where participants dressed in Ku Klux Klan-type outfits gave greater shocks than participants dressed in nurse outfits). Thus, groups are more vicious when they believe their victims cannot retaliate against them. See Tizra Leader, Brian Mullen & Dominic Abrams, *Without Mercy: The Immediate Impact of Group Size on Lynch Mob Atrocity*, 33 *PERSONALITY & SOC. PSYCHOL. BULL.* 1340, 1342 (2007).

¹⁶² Zimbardo, *supra* note 161, at 296 (explaining how Nazis dehumanized the Jews during the Holocaust); see Roberta Senechal de la Roche, *The Sociogenesis of Lynching*, in *UNDER SENTENCE OF DEATH: LYNCHING IN THE SOUTH* 48, 55-56 (W. Fitzhugh Brundage ed., 1997) (explaining that lynching incidents were more prevalent and violent when the victim was a stranger to the community).

members feel free to attack without regret.¹⁶³ Groups rarely target those who are important to their personal well-being.¹⁶⁴ For instance, the incidence of lynching in the South similarly tracked the degree of interdependence between victims and the violent crowd, with black newcomers more vulnerable to violence than black employees who worked for the white community.¹⁶⁵

Lastly, group members are more aggressive if they sense that authority figures support their efforts. Social scientists emphasize a perceived leader's role in accelerating dangerous group behavior.¹⁶⁶ As recently as the early 1900s, Southern newspapers explicitly "legitimated mob violence" by reporting that lynch mobs included prominent members of the white community.¹⁶⁷ As legal historian Robert Kaczorowski explains, federal authorities implicitly encouraged the Klan by failing to enforce civil rights laws.¹⁶⁸

The Internet magnifies the dangerousness of group behavior in each of these respects. Web 2.0 platforms create a feeling of closeness among like-minded individuals.¹⁶⁹ Online groups affirm each other's negative views, which become more extreme and destructive.¹⁷⁰ Individuals say and do things online they would never consider saying or doing offline because they feel anonymous, even if they write under their real names.¹⁷¹ Because group

¹⁶³ Senechal de la Roche, *supra* note 162, at 55-56.

¹⁶⁴ Roberta Senechal de la Roche, *Collective Violence as Social Control*, 11 SOC. F. 97, 106-07 (1996).

¹⁶⁵ *Id.*; see W. FITZHUGH BRUNDAGE, *LYNCHING IN THE NEW SOUTH: GEORGIA AND VIRGINIA, 1880-1930*, at 81-82 (1993) (describing how whites feared that black floaters "posed a continual threat to white women and children").

¹⁶⁶ David R. Mandel, *Evil and the Instigation of Collective Violence*, 2002 ANALYSES SOC. ISSUES & PUB. POL'Y 101, 102.

¹⁶⁷ STEWART E. TOLNAY & E.M. BECK, *A FESTIVAL OF VIOLENCE: AN ANALYSIS OF SOUTHERN LYNCHINGS, 1882-1930*, at 25-27 (1995).

¹⁶⁸ ROBERT J. KACZOROWSKI, *THE POLITICS OF JUDICIAL INTERPRETATION: THE FEDERAL COURTS, DEPARTMENT OF JUSTICE, AND CIVIL RIGHTS, 1866-1876*, at 66 (2005).

¹⁶⁹ See PATRICIA WALLACE, *THE PSYCHOLOGY OF THE INTERNET* 79 (1999); Katelyn Y.A. McKenna & Amie S. Green, *Virtual Group Dynamics*, 6 GROUP DYNAMICS 116, 116, 120 (2002).

¹⁷⁰ WALLACE, *supra* note 169, at 79.

¹⁷¹ *Id.* at 125 (reporting a study in which anonymous Internet conferencing groups experienced six times as many uninhibited hostile remarks as non-anonymous groups); Russell Spears et al., *De-individuation and Group Polarization in Computer-Mediated Communication*, 29 BRIT. J. SOC. PSYCHOL. 121, 122-24 (1990) (reviewing research that attempts to explain the "risky shift effect," in which group discussions veer toward extreme positions, as a product of visual anonymity). Computer-mediated interactions inevitably engender feelings of anonymity. ADAM N. JOINSON, *UNDERSTANDING THE PSYCHOLOGY OF INTERNET BEHAVIOUR: VIRTUAL WORLDS, REAL LIVES* 23 (2003). Such communications are conducted in a state of visual anonymity as users cannot see those with whom they are

members often shroud themselves in pseudonyms, they have little fear that victims will retaliate against them or that they will suffer social stigma for their abusive conduct. Online groups also perceive their victims as “images” and thus feel free to do anything they want to them.¹⁷²

Moreover, site operators who refuse to dismantle damaging posts reinforce, and effectively encourage, negative behavior.¹⁷³ Their refusal can stem from a libertarian “You Own Your Own Words” philosophy¹⁷⁴ or irresponsibility, bred from the belief they enjoy broad statutory immunity from liability.¹⁷⁵ Negative posts that remain online constitute “calls to action” that generate others in a “snowball effect.”¹⁷⁶

II. THE COMPONENTS OF CYBER CIVIL RIGHTS STRATEGY

Because destructive online mobs are unlikely to correct themselves, a comprehensive legal response is essential to deter and redress the harm they cause.¹⁷⁷ Much like its forebears, a cyber civil rights agenda must begin with the courts, because legislatures and executives have yet to respond to abusive online mobs in a comprehensive manner.¹⁷⁸ Professor Derrick Bell has

communicating. *Id.* Even if users see an individual’s e-mail address, name, or familiar pseudonym, such “identifiability” is not equivalent to meeting someone in person. *Id.*

¹⁷² Teresa Wiltz, *Cyberspace Shields Hateful Bloggers*, J. GAZETTE (Fort Wayne), Nov. 17, 2007, at 2D, available at <http://www.journalgazette.net/apps/pbcs.dll/article?AID=/20071117?ENT/711170381&te> (quoting John Perry Barlow).

¹⁷³ SOLOVE, *supra* note 4, at 159.

¹⁷⁴ For instance, Chris Locke, the operator of the sites involved in the Kathy Sierra attacks, explained that he initially did not take down the posts about Ms. Sierra due to his libertarian philosophy. Jim Turner, *supra* note 18.

¹⁷⁵ SOLOVE, *supra* note 4, at 159 (claiming that 47 U.S.C. § 230 (2000) encourages irresponsible online behavior by too broadly immunizing bloggers from liability for user-posted content).

¹⁷⁶ Amanda Paulson, *Internet Bullying*, CHRISTIAN SCI. MONITOR, Dec. 23, 2003, at 11; Dahlia Lithwick, *Fear of Blogging: Why Women Shouldn’t Apologize for Being Afraid of Threats on the Web*, SLATE, May 4, 2007, <http://www.slate.com/toolbar.aspx?action=print&id=2165654> (suggesting that online threats combined with postings of the victim’s home address and Social Security number provide incitement to deranged third parties); see *High-Tech Bullying is Sweeping the Nation*, KENT & SUSSEX COURIER (U.K.), Sept. 8, 2006, at 10 (describing the snowball effect of harassing message board posts and mobile phone texts that escalate bullying and threats aimed at victims).

¹⁷⁷ See SOLOVE, *supra* note 4, at 190 (discussing how a libertarian approach to address online attacks on reputation is unacceptable given the threat to privacy caused by the increasing spread of online information and the unlikelihood of market correction).

¹⁷⁸ See DERRICK BELL, AND WE ARE NOT SAVED: THE ELUSIVE QUEST FOR RACIAL JUSTICE 59 (1987) [hereinafter BELL, WE ARE NOT SAVED] (explaining that because legislatures and executives were unresponsive to civil rights issues, groups fighting for

counseled that civil rights progress is most likely to occur when the interests of vulnerable people can be aligned with those of the dominant group.¹⁷⁹ Section A heeds that advice, demonstrating that society as a whole suffers much due to online attacks and proposing remedies under criminal statutes and general tort doctrines.

On the other hand, online attacks are fundamentally civil rights violations and, in many respects, mirror activities that prompted enactment of prior centuries' civil rights laws. Accordingly, Section B shows how civil rights laws fill critical gaps left by traditional tort and criminal law in combating the individual and societal harm that online mobs inflict.

A. *Converging the Interests of the Majority with Those of Subjugated Groups*

1. Broader Societal Harm Wrought by Online Mobs

Although online mobs typically focus on women, people of color, and other traditionally subjugated groups, they harm society at large. When mobs succeed in their professed goal of driving bloggers offline, or of using online attacks to silence their victims' offline speech, they impoverish the dialogue society depends upon for purposes great and small. The attacks on Kathy Sierra deprived society of an apparently talented and enthusiastic blogger on software design.¹⁸⁰

The proliferation of sexual threats and violent sexual imagery on websites not otherwise devoted to such material increases the likelihood that children and unwilling adults will encounter it. As such material becomes increasingly difficult to avoid, increasing numbers of parents will restrict or deny their

racial justice such as the NAACP relied on the courts as a matter of necessity). Professor Bell analogized civil rights litigation to "a leaky boat that one paddles through treacherous waters." Derrick Bell, *Foreword: The Civil Rights Chronicles*, 99 HARV. L. REV. 4, 35-36 (1985). As Bell suggests, pursuing civil rights litigation is essential until a better option presents itself. *Id.* at 36.

¹⁷⁹ BELL, WE ARE NOT SAVED, *supra* note 178, at 63-74 (explaining that progress on racial issues depends on the ability to convince whites that they will benefit from a social justice agenda); Derrick A. Bell, Jr., Comment, *Brown v. Board of Education and the Interest Convergence Dilemma*, 93 HARV. L. REV. 518, 523 (1980), *reprinted in* CRITICAL RACE THEORY: THE KEY WRITINGS THAT FORMED THE MOVEMENT 20, 22 (Kimberlé Crenshaw et al. eds., 1995) [hereinafter Bell, *Interest Convergence*]. Professor Bell contends that "the Fourteenth Amendment, standing alone, will not authorize a judicial remedy providing effective racial equality for blacks where the remedy sought threatens the superior societal status of middle- and upper-class whites." Bell, *Interest Convergence*, *supra*, at 22; *see also* Richard Delgado & Jean Stefancic, *Introduction to CRITICAL RACE THEORY: THE CUTTING EDGE*, at xvi-xvii (Richard Delgado & Jean Stefancic eds., 2d ed. 2000) ("Because racism is an ingrained feature of our landscape, it looks ordinary and natural to persons in the culture. . . . [W]hite elites will tolerate or encourage racial advances for blacks only when such advances also promote white self-interest.").

¹⁸⁰ *See supra* notes 12-22 and accompanying text.

children's web access and other adults will turn away from the Internet in disgust. Moreover, when online mobs post Social Security numbers and other information to facilitate identity theft, they increase the receipts of identity theft rings and spread costs throughout the financial sector. Their dissemination of disinformation about potential employees in a manner that as a practical matter is impossible to refute distorts the employment market.¹⁸¹

On a more granular level, support for this proposal will extend beyond those interested in protecting individuals from traditionally disadvantaged groups because the traditional criminal and tort law doctrines featured here can be invoked by individuals from dominant groups who have been attacked online. Examples of such online harassment abound. For instance, in the summer of 2008, a man sought to ruin the reputation of an investment banker, Steven Rattner, who allegedly had an affair with the man's wife.¹⁸² On six websites, the man accused Mr. Rattner of trying to "steal" the man's wife with exotic trips and expensive gifts.¹⁸³ He included these accusations in e-mails to Mr. Rattner's colleagues, clients, and reporters.¹⁸⁴ Although Mr. Rattner admits having the affair, he says the man's other claims are "either untrue or a gross exaggeration."¹⁸⁵ The online accusations spread like a virus, forcing Mr. Rattner to resign from his job.¹⁸⁶ This example shows that because online attacks harm not only vulnerable individuals like women and minorities, but also individuals from dominant groups like Mr. Rattner, one can expect widespread support for the application of general tort and criminal law remedies for online assaults.

2. Traditional Tort and Criminal Laws That Should Be Invoked to Combat Cyber Harassment

Traditional criminal prosecutions and tort suits should be pursued to deter and remedy an online mob's assaults.¹⁸⁷ Prosecutors can pursue online mobs for computer-related crimes,¹⁸⁸ such as hacking into a victim's computers and password-protected accounts¹⁸⁹ or disseminating denial-of-service and "image

¹⁸¹ Even if the mobs' accusations are only modestly persuasive, risk-averse employers may select other candidates.

¹⁸² Andrew Ross Sorkin, *On Wall St., Reputation Is Fragile*, N.Y. TIMES, Aug. 5, 2008, at C1.

¹⁸³ *Id.*

¹⁸⁴ *Id.*

¹⁸⁵ *Id.*

¹⁸⁶ *Id.*

¹⁸⁷ This Article does not catalogue every possible traditional tort or crime implicated by the attacks of online mobs. Instead, it offers examples of traditional legal remedies that might be pursued against online mobs.

¹⁸⁸ Xiaomin Huang et al., *Computer Crimes*, 44 AM. CRIM. L. REV. 285, 298-92 (2007).

¹⁸⁹ 18 U.S.C. § 1030(a)(2)(C) (2000) (punishing the intentional access of a computer without authorization to obtain information); *id.* § 1030(a)(4) (prohibiting unauthorized

reaping” attacks to shut down blogs and websites.¹⁹⁰ They can also prosecute cyber mobs under 18 U.S.C. § 875(c) for online threats of rape, strangulation, and other physical harm if victims could have reasonably believed that those threatening them expressed a serious intent to inflict bodily harm.¹⁹¹ Further, prosecutors could charge an individual with the intent to aid and abet identity theft for the posting of Social Security numbers.¹⁹² In addition to criminal prosecutions, victims can bring civil causes of action based on any of the computer-related crimes discussed above.¹⁹³

Targeted individuals could also pursue general tort claims, such as defamation.¹⁹⁴ False statements and distorted pictures that disgrace plaintiffs or injure their careers constitute defamation per se, for which special damages

access of a protected computer where the perpetrator intends to fraudulently obtain something of value); *see, e.g.*, *United States v. Ivanov*, 175 F. Supp. 2d 367, 371 (D. Conn. 2001) (holding that stealing credit card numbers from a computer amounted to theft of something valuable under § 1030(a)(4)). Computer hackers have been prosecuted for stealing a variety of sensitive personal information, from credit card numbers to medical data. *E.g.*, *Selling Singer’s Files Gets Man Six Months*, HOUSTON CHRON., Dec. 2, 2000, at A2; Press Release, U.S. Dep’t of Justice, Russian Computer Hacker Sentenced to Three Years in Prison (Oct. 4, 2002), *available at* <http://www.cybercrime.gov/gorshkovSent.htm>.

¹⁹⁰ 18 U.S.C. § 1030(a)(5) (imposing criminal sanctions for knowingly causing the transmission of a program, code, or command that causes damage to computers); 18 U.S.C. § 1030(e) (stating that victims need only suffer impairment to integrity or availability of data, programs, systems, or information to sustain a § 1030(a)(5) conviction).

¹⁹¹ Section 875(c) prohibits the transmission “in interstate or foreign commerce” of communications that contain threats to injure another person. 18 U.S.C. § 875(c) (2000); *see, e.g.*, *United States v. Teague*, 443 F.3d 1310, 1317 (10th Cir. 2006). Similarly, many states have some form of assault law that proscribes the use of words to create fear of harm in a victim. *See* KENT GREENAWALT, SPEECH, CRIME, AND THE USES OF LANGUAGE 90-104 (1989). In the AutoAdmit case, the targeted individuals could have reasonably believed that those threatening them meant to express a serious intent to inflict bodily harm and had the ability to carry out the attacks where the posts detailed their home addresses, clothing, and schedule, suggesting the poster’s close proximity. *See supra* notes 54-87 and accompanying text (summarizing AutoAdmit postings that described female student’s attire, suggesting contact with targeted women, and warned of rape).

¹⁹² The Identity Theft Assumption Deterrence Act of 1998 outlaws the knowing transfer or use of another person’s means of identification with the intent to commit or to aid or abet unlawful activity. 18 U.S.C. § 1028(a)(7) (2000). Courts have upheld convictions for aiding and abetting identity theft in cases where defendants posted Social Security numbers, home addresses, and driver’s licenses online for identity thieves to use. *United States v. Sutcliffe*, 505 F.3d 944, 950-52, 959-60 (9th Cir. 2007).

¹⁹³ 18 U.S.C. § 1030(g) (2000); *Fiber Sys. Int’l, Inc. v. Roehrs*, 470 F.3d 1150, 1155-56 (5th Cir. 2006).

¹⁹⁴ *Cf.* LAWRENCE M. FRIEDMAN, GUARDING LIFE’S DARK SECRETS: LEGAL AND SOCIAL CONTROLS OVER REPUTATION, PROPRIETY, AND PRIVACY 43, 235 (2007).

need not be proven.¹⁹⁵ Numerous statements and pictures described in Part I, if indeed false, provide grounds for defamation claims as they degrade societal perceptions of the targeted individuals.¹⁹⁶

Victims could sue for public disclosure of private facts. The public-disclosure-of-private-facts tort involves the publicity of private, non-newsworthy information, disclosure of which would be “highly offensive to a reasonable person.”¹⁹⁷ The tort’s applicability seems clear for an online mob’s publication of a plaintiff’s Social Security number; such a release would offend the reasonable person given the concomitant risk of identity theft.¹⁹⁸

Many victims may have actions for intentional infliction of emotional distress. That tort responds to “extreme and outrageous conduct” by a defendant who intended to cause, or recklessly caused, the plaintiff’s severe emotional distress.¹⁹⁹ Courts are more willing to consider conduct “outrageous” if the defendant exploited an existing power disparity between the parties or knowingly took advantage of a vulnerable plaintiff.²⁰⁰ Various types of online harassment have supported emotional distress claims, including threats of violence, the publication of a victim’s sensitive information, and disparaging racial remarks.²⁰¹ Victims can certainly argue that many of the

¹⁹⁵ See, e.g., *Kiesau v. Bantz*, 686 N.W.2d 164, 169-70, 178 (Iowa 2004) (upholding a finding of libel per se where the defendant altered a photograph of a female police officer to make it appear that she intentionally exposed her breasts and e-mailed the picture to plaintiff’s colleagues); *Rombom v. Weberman*, No. 1378/00, 2002 WL 1461890, at *2 (N.Y. Sup. Ct. June 13, 2002) (upholding a defamation award based on defamatory per se for online postings asserting the plaintiff was a “pathological liar,” a psychopath, a burglar, and a kidnapper).

¹⁹⁶ See *supra* text accompanying notes 16, 18, 65-73, 80, 81, 95, 97, 119.

¹⁹⁷ RESTATEMENT (SECOND) OF TORTS § 652D (1977); see DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 101-06 (2008).

¹⁹⁸ See *supra* note 15 and accompanying text (discussing the release of Ms. Sierra’s Social Security number).

¹⁹⁹ RESTATEMENT (SECOND) OF TORTS § 46(1) (1965).

²⁰⁰ *Id.* § 46 cmts. e-f (1965); see, e.g., *Inland Mediation Bd. v. City of Pomona*, 158 F. Supp. 2d 1120, 1132, 1156-57 (C.D. Cal. 2001) (upholding emotional distress claim based on defendant’s public comment that he refused to rent to Blacks because they “were nothing but trouble” and engaged in criminal behavior on the grounds that a jury “may consider a plaintiff’s race in evaluating the plaintiff’s susceptibility to emotional distress resulting from discriminatory conduct”).

²⁰¹ See, e.g., *Gonsalves v. Consecro Ins. Co.*, No. Civ. S-06-0058 WBS KJM, 2006 WL 3486962, at *6 (E.D. Cal. Dec. 1, 2006) (denying the defendant’s motion for summary judgment on a claim of intentional infliction of emotional distress because a reasonable jury could find that posting the plaintiff’s name and Social Security number on a website amounted to extreme and outrageous conduct); *State v. Carpenter*, 171 P.3d 41, 58 (Alaska 2007) (holding the defendant radio announcer’s actions could constitute extreme and outrageous conduct because he gave his audience the plaintiff’s telephone and fax numbers and urged the audience to make the plaintiff’s life “a living hell”); *Delfino v. Agilent Techs., Inc.*, 52 Cal. Rptr. 3d 376, 382 n.6, 392 (2006) (concluding that “odious e-mail

assaults featured in Part I constitute “extreme and outrageous” conduct and caused severe emotional distress, as nearly all of them involved gruesome threats of physical violence and other forms of harassment.²⁰²

Some victims may also bring actions for intrusion on seclusion. This tort protects against intentional intrusions into a person’s “private affairs or concerns” if the intrusions would be “highly offensive to a reasonable person.”²⁰³ Courts have upheld intrusion claims for deliberate interruptions of a person’s online activities.²⁰⁴ Online mobs could face intrusion claims for hacking into password protected e-mail accounts containing private correspondence and conducting denial-of-service attacks to shut down personal blogs and websites.²⁰⁵

B. *A Crucial Deterrent and Remedy for Cyber Harassment of Vulnerable Individuals: Civil Rights Law*

A meaningful response to abusive online mobs would include the enforcement of existing civil rights laws for several reasons. First, civil rights laws recognize the serious injuries that online mobs inflict on victims, their communities, and society as whole.²⁰⁶ Cyber attacks marginalize individuals belonging to traditionally subordinated groups, causing them deep psychological harm.²⁰⁷ Victims feel helpless to avoid future attacks because they are unable to change the characteristic that made them victims.²⁰⁸ They experience feelings of inferiority, shame, and a “profound sense of isolation.”²⁰⁹ The attacks perpetrate economic intimidation and suppress civic

messages and postings” threatening, “[y]ou can look forward to all your fingers getting broken, several kicks to the ribs and mouth, break some teeth [sic], and a cracked head,” may constitute extreme and outrageous acts).

²⁰² See *supra* text accompanying notes 15, 20-22, 86 (describing Kathy Sierra’s response to online threats, the emotional distress alleged by AutoAdmit plaintiffs, and online postings of victims’ Social Security numbers).

²⁰³ RESTATEMENT (SECOND) OF TORTS § 652B (1977).

²⁰⁴ See, e.g., *Donnel v. Lara*, 703 S.W.2d 257, 260 (Tex. Ct. App. 1985) (recognizing an intrusion claim where a creditor made intrusive phone calls to the plaintiff).

²⁰⁵ See *supra* notes 90, 106, 115 and accompanying text (describing a mob’s conduct of hacking into a woman’s e-mail, Facebook, and MySpace accounts to obtain her passwords and sensitive personal information and detailing denial-of-service and “image reaping” attacks).

²⁰⁶ Frederick M. Lawrence, *The Evolving Federal Role in Bias Crimes Law Enforcement and the Hate Crimes Prevention Act of 2007*, 19 STAN. L. & POL’Y REV. 251, 255-59 (2008) [hereinafter Lawrence, *Evolving Role*].

²⁰⁷ See Joshua Cohen, *Freedom of Expression*, 22 PHIL. & PUB. AFF. 207, 255-57 (1993).

²⁰⁸ FREDERICK M. LAWRENCE, PUNISHING HATE: BIAS CRIMES UNDER AMERICAN LAW 40 (1999) [hereinafter LAWRENCE, PUNISHING HATE].

²⁰⁹ *Id.* at 40-41; Lawrence, *Evolving Role*, *supra* note 206, at 255. Charles Lawrence distinguishes racist speech from other offensive words because they “evoke in you all of the millions of cultural lessons regarding your inferiority that you have so painstakingly

engagement, depriving vulnerable individuals of their equal right to participate in social, economic, and political life.²¹⁰

Bias-motivated conduct also provokes retaliation and incites community unrest.²¹¹ Such attacks also harm the community that shares the victim's race, gender, religion, or ethnicity – community members experience attacks as if the attacks happened to them.²¹² Moreover, society suffers when victims and community members isolate themselves to avoid future attacks and when cyber mobs violate our shared values of equality and pluralism.²¹³ Traditional tort and criminal law fail to respond to such systemic harm and, indeed, may obscure a full view of the damage.

Second, a civil rights approach would play a valuable normative and expressive role in society.²¹⁴ Civil rights prosecutions would communicate society's commitment to "values of equality of treatment and opportunity" and make clear that conduct transgressing those values will not be tolerated.²¹⁵

repressed, and imprint upon you a badge of servitude and subservience for all the world to see." Charles R. Lawrence III, *If He Hollers Let Him Go: Regulating Racist Speech on Campus*, 1990 DUKE L.J. 431, 461.

²¹⁰ See KENNETH L. KARST, *BELONGING TO AMERICA: EQUAL CITIZENSHIP AND THE CONSTITUTION* 13 (1989); ANDREW KOPPELMAN, *ANTIDISCRIMINATION LAW AND SOCIAL EQUALITY* 57-114 (1996) (summarizing arguments that a central purpose of antidiscrimination law is to remedy the stigmatization that deprives individuals of equal participation in society).

²¹¹ See Lawrence, *Evolving Role*, *supra* note 206, at 258 & n.20 (describing the Crown Heights riots, in which "the mere perception of a bias crime" provoked several days of retaliation and community unrest).

²¹² See *id.* at 257-58.

²¹³ LAWRENCE, *PUNISHING HATE*, *supra* note 208, at 43-44.

²¹⁴ See Deborah Hellman, *The Expressive Dimension of Equal Protection*, 85 MINN. L. REV. 1, 2, 30, 37 (2000) (exploring the expressive dimension of law in equality jurisprudence and articulating an expressivist theory of Equal Protection, namely that "state action violates Equal Protection if its *meaning* conflicts with the government's obligation to treat each person with equal concern"). A compelling body of literature addresses the merits of expressivist conceptions of law more generally. *Id.* at 28-37. See generally Matthew D. Adler, *Expressive Theories of Law: A Skeptical Overview*, 148 U. PA. L. REV. 1363 (2000) (concluding that expressive theories of the law are unpersuasive because adherents confuse "social meaning" with linguistic meaning); Richard H. Pildes, *Why Rights Are Not Trumps: Social Meanings, Expressive Harms, and Constitutionalism*, 27 J. LEGAL STUD. 725 (1998) (espousing the importance of the "expressive dimension of governmental action" in constitutional law as a foil to Dworkin's conception of rights as "trumps" that protect individual interests contrary to the common good).

²¹⁵ LAWRENCE, *PUNISHING HATE*, *supra* note 208, at 167-69.

They also would be a powerful stigmatizing tool²¹⁶ because the fear of censure might inhibit abusive behavior.²¹⁷

Third, viewing the assaults as civil rights violations might provide an incentive for prosecutors to pursue criminal charges. To date, law enforcement's response to online criminal activities has evolved slowly.²¹⁸ Computer crimes are difficult to prosecute given law enforcement's relative unfamiliarity with technology.²¹⁹ Prosecutors might devote more resources to untangling a case's difficult technological issues if they recognized its civil rights implications.

Fourth, civil rights laws have attractive remedial features. Because damages may be hard to prove and quantify, and because many plaintiffs cannot afford to litigate based on principle alone, the high cost of litigation often deters the filing of general tort suits.²²⁰ The awards of attorney's fees possible under many civil rights statutes might make some cases affordable to pursue.

Fifth, civil rights suits may reach wrongs that would otherwise escape liability. These include victims' rights to be free from economic intimidation and cyber harassment based on race and gender.

Finally, civil rights law has adapted over the years to many of the conditions that exacerbate the extreme behavior of online mobs.²²¹ It has had to respond to hateful mobs emboldened by anonymity. It also has confronted the objectification of subordinated people, a process the Internet fosters by disaggregating people into screen presences that mob members can attack as if playing a computer game.

1. Common Civil Rights Doctrines

Online assaults motivated by race discrimination that interfere with an individual's ability to make a living can support civil and criminal actions.²²² 42 U.S.C. § 1981 guarantees members of racial minorities "the same right in every State . . . to make and enforce contracts . . . as is enjoyed by white

²¹⁶ See Dan M. Kahan, *What Do Alternative Sanctions Mean?*, 63 U. CHI. L. REV. 591, 592 (1996) (explaining the expressive and normative importance of imprisonment as symbolizing moral condemnation).

²¹⁷ See Cass R. Sunstein, *On the Expressive Function of Law*, 144 U. PA. L. REV. 2021, 2029-36 (1996). Of course, the tort remedies and criminal prosecutions discussed above also play an important expressive and normative role. See *supra* Part II.A.2.

²¹⁸ Smith, *supra* note 51, at 28.

²¹⁹ Huang et al., *supra* note 188, at 315-16.

²²⁰ See Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 DUKE L.J. 855, 872-76 (2000).

²²¹ See *supra* Part I.B.

²²² This Section focuses on federal civil rights legislation, both criminal and civil, which often parallel laws on the state level.

citizens”²²³ A plaintiff must show that the defendant intended to discriminate on the basis of race and that the discrimination concerned the “making and enforcement” of contracts.²²⁴ Courts have upheld § 1981 damages in cases where masked mob members used tactics of intimidation to prevent members of racial minorities from “making a living” in their chosen field.²²⁵ Section 1981 remedies “purely private” acts of racial discrimination and thus does not require state action.²²⁶

Similarly, 18 U.S.C. § 245(b)(2)(C), a provision of the Civil Rights Act of 1968, criminalizes “force or threat[s] of force” designed to intimidate or interfere with a person’s private employment due to that person’s race, religion, or national origin.²²⁷ Congress enacted § 245 to rid interstate commerce of the burdens imposed by denying persons equal employment opportunities and other federally protected activities through threats of violence.²²⁸ Courts have upheld § 245 prosecutions where defendants threatened violence over employees’ e-mail and voicemail.²²⁹

Gender discrimination that interferes with a person’s ability to make a living can be pursued under Title VII of the Civil Rights Act of 1964, which sanctions those who intimidate, threaten, or coerce, or attempt to intimidate, threaten, or coerce someone with the purpose of interfering with employment

²²³ 42 U.S.C. § 1981 (2000); *Saint Francis Coll. v. Al-Khazraji*, 481 U.S. 604, 609 (1987). Section 1981 was enacted under the Thirteenth Amendment, which allowed Congress to rationally determine the badges and incidents of slavery and to translate them into effective legislation. *Runyon v. McCrary*, 427 U.S. 160, 170 (1976). People who are protected by the statute include those who “are subjected to intentional discrimination solely because of their ancestry or ethnic characteristics.” *Al-Khazraji*, 481 U.S. at 613.

²²⁴ *Morris v. Office Max, Inc.*, 89 F.3d 411, 413 (7th Cir. 1996). The “mak[ing] and enforce[ment of] contracts” is defined as “the making, performance, modification, and termination of contracts, and the enjoyment of all benefits, privileges, terms and conditions of the contractual relationship.” 42 U.S.C. § 1981(b).

²²⁵ *E.g.*, *Vietnamese Fishermen’s Ass’n v. Knights of the Ku Klux Klan*, 518 F. Supp. 993, 1001-04, 1008, 1016-17 (S.D. Tex. 1981) (upholding a judgment in a § 1981 case where hooded Klan members threatened violence and burned crosses to prevent Vietnamese fishermen from fishing in Gulf waters which held plaintiffs had a protected interest in making a living free from racial animus).

²²⁶ *Patterson v. McLean Credit Union*, 491 U.S. 164, 185 (1989); *Runyon*, 427 U.S. at 170.

²²⁷ 18 U.S.C. § 245(b)(2)(C) (2000). “The statutory language that eventually became § 245 originated in Title V of the proposed Civil Rights Act of 1966.” *United States v. Lane*, 883 F.2d 1484, 1489 n.8 (10th Cir. 1989).

²²⁸ *Lane*, 883 F.2d at 1492-93 (holding that § 245(b)(2)(C) could be applied in the race-motivated murder of a Jewish radio talk show host because Congress may, in a valid exercise of its Commerce Clause power, “prohibit a person from denying another person equal employment opportunities because of his race by violently injuring or killing him”).

²²⁹ *United States v. Syring*, 522 F. Supp. 2d 125, 126 (D.D.C. 2007).

opportunities due to their gender.²³⁰ The Attorney General can file civil suits for injunctive relief.²³¹ Such actions can be asserted against private actors because Congress enacted Title VII of the Civil Rights Act of 1964 pursuant to a valid exercise of its power to regulate interstate commerce.²³² Courts have upheld Title VII violations where masked defendants engaged in “economic coercion” and intimidation to prevent vulnerable individuals from employment.²³³

Destructive online crowds intimidate women and members of racial and religious minorities, preventing them from “making a living” due to discriminatory animus. Because the Internet fuses our public and private lives and is a workplace for many, online attacks on vulnerable individuals often interfere with their equal right to pursue work. For instance, women who stop blogging in the face of an online mob’s attack lose advertising revenue and opportunities for advancement.²³⁴ According to technology blogger Robert Scoble, women who lack a robust online presence are “never going to be included in the [technology] industry.”²³⁵ Online mobs also conduct denial-of-service attacks to shut down blogs that generate income for women and racial minorities. They spread damaging statements to employers and professors for whom victims may work in order to interfere with their employment opportunities.

Online mob attacks also implicate state laws penalizing those who harass or stalk another by communicating words, images, or language through electronic mail or the Internet, directed to a specific person, which would cause a reasonable person substantial emotional distress or fear of bodily harm.²³⁶

²³⁰ 42 U.S.C. § 2000e-2 (2000).

²³¹ *Id.* § 2000e-6.

²³² *United States v. Original Knights of Ku Klux Klan*, 250 F. Supp. 330, 349 (E.D. La. 1965); *see Heart of Atlanta Motel, Inc. v. United States*, 379 U.S. 241, 250 (1964); *Katzenbach v. McClung*, 379 U.S. 294, 304 (1964).

²³³ *Original Knights of Ku Klux Klan*, 250 F. Supp. at 356.

²³⁴ *See Nakashima*, *supra* note 9.

²³⁵ *Id.*

²³⁶ *See, e.g., CAL. PENAL CODE § 653m(b)* (West 1999); *FLA. STAT. ANN. § 784.048* (West 2007). Typically, the mens rea for cyber stalking crimes is the intent to engage in conduct that causes the targeted individual to fear for her safety or suffer severe emotional distress. Naomi Harlin Goodno, *Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 MO. L. REV. 125, 133-34 (2007). Forty-six stalking and harassment state statutes have withstood vagueness and overbreadth challenges. *See, e.g., State v. Richards*, 896 P.2d 357, 359-60 (Idaho Ct. App. 1995); *Commonwealth v. Hendrickson*, 724 A.2d 315, 319 (Pa. 1999). States such as Oregon revised harassment laws that were struck down on vagueness and overbreadth grounds. *Compare State v. Sanderson*, 575 P.2d 1025, 1027 (Or. Ct. App. 1978) (en banc) (striking down a harassment statute because the phrase “alarms or seriously annoys” was too vague), *with State v. Maxwell*, 998 P.2d 680, 684-86 (Or. Ct. App. 2000) (upholding a stalking conviction against a challenge

Some states explicitly criminalize posting messages with the intent to urge or incite others to harass a particular individual.²³⁷ For instance, California authorities obtained a guilty plea from a defendant who terrorized a victim by impersonating her in chat rooms and online bulletin boards, where the defendant posted the victim's home address and messages suggesting the victim fantasized about being raped.²³⁸

2. Civil Rights Doctrines Focusing on Anonymous Attackers

Civil rights law has long recognized the dangers that anonymous mobs pose. Title 42 U.S.C. § 1985(3) allows damage suits against:

[T]wo or more persons in any State or Territory [who] conspire or go in disguise on the highway or on the premises of another, for the purpose of depriving, either directly or indirectly, any person or class of persons of the equal protection of the laws, or of equal privileges and immunities under the laws; or for the purpose of preventing or hindering the constituted authorities of any State or Territory from giving or securing to all persons within such State or Territory the equal protection of the laws²³⁹

To similar effect, § 241 establishes criminal penalties for “two or more persons [who] go in disguise on the highway, or on the premises of another, with intent to prevent or hinder his free exercise or enjoyment of any right or privilege” that is “secured to him by the Constitution or laws of the United States, or because of his having so exercised the same.”²⁴⁰

Online mobs go in disguise on the Internet for the admitted purpose of suppressing the free speech of victims expressly targeted because they are women, people of color, members of religious minorities, or gays or lesbians. Sections 1985 and 241 similarly proscribe conspiracies to deprive others of civil rights.²⁴¹ Section 1986 then establishes a cause of action against any person, “having knowledge that any of the wrongs conspired to be done, and

that the statutory term “visual or physical presence” was unconstitutionally vague under the Oregon Constitution).

²³⁷ *E.g.*, OHIO REV. CODE ANN. § 2903.21.1(A)(1)-(2) (LexisNexis Supp. 2008).

²³⁸ U.S. DEP'T OF JUSTICE, 1999 REPORT ON CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY (1999), *available at* <http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm>. Part I documents examples of such online harassment and stalking of women and people of color.

²³⁹ 42 U.S.C. § 1985(3) (2000).

²⁴⁰ 18 U.S.C. § 241 (2000).

²⁴¹ Section 1985(3) simply creates a cause of action against conspiracies with any of the same objects proscribed for persons going in disguise. 42 U.S.C. § 1985(3). Section 241 criminalizes “conspir[acies] to injure, oppress, threaten, or intimidate any person in [the United States] in the free exercise or enjoyment of any right or privilege secured to him by the Constitution or laws of the United States, or because of his having so exercised the same” 18 U.S.C. § 241.

mentioned in section 1985 . . . are about to be committed,” who could have helped prevent those acts from being committed but who fails to do so.²⁴²

Efforts to apply these statutes to anonymous online mobs nonetheless face formidable obstacles. During Reconstruction, *United States v. Cruikshank* interpreted the language of the Enforcement Act, which included much of the language later incorporated into § 1985(3), as not reaching purely private conspiracies, and suggested Congress lacked the authority to go farther.²⁴³ Almost one hundred years later, the Court found that Congress could reach some purely private conspiracies through its powers to implement the Thirteenth Amendment and to protect the right to interstate travel.²⁴⁴ More recently, however, the Court narrowed the statute’s reach, finding it only covers private conspiracies “‘aimed at interfering with rights’ that are ‘protected against private, as well as official, encroachment.’”²⁴⁵ The Court held that freedom of speech is not such a right.²⁴⁶

The Court noted that the Commerce Clause “no doubt” allowed Congress to proscribe private efforts to prevent the exercise of speech or rights secured only against state interference, but held “§ 1985(3) is not such a provision” because of its references to “rights, privileges, and immunities” under the laws.²⁴⁷ Whatever one may think of this interpretation, Congress has since enacted such a law. The Violence Against Women Act (“VAWA”) penalizes anyone who “utilizes a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with the intent to annoy, abuse, threaten or harass any person at the called number or who receives communications” with fines or imprisonment.²⁴⁸ A telecommunications device is defined to include “any device or software that can be used to originate telecommunications or other types of communications

²⁴² 42 U.S.C. § 1986.

²⁴³ *United States v. Cruikshank*, 92 U.S. 542, 554-55 (1875).

²⁴⁴ *Griffin v. Breckenridge*, 403 U.S. 88, 104-06 (1971).

²⁴⁵ *Bray v. Alexandria Women’s Health Clinic*, 506 U.S. 263, 268 (1993) (quoting *United Bhd. of Carpenters Local 610 v. Scott*, 463 U.S. 825, 833 (1983)). The Court also suggested “it is a close question whether § 1985(3) was intended to reach any class-based animus other than animus against Negroes and those who championed their cause . . .” *United Bhd. of Carpenters Local 610*, 163 U.S. at 836.

²⁴⁶ *United Bhd. of Carpenters Local 610*, 163 U.S. at 830.

²⁴⁷ *Id.* at 833.

²⁴⁸ 47 U.S.C.A. § 223(a)(1)(C) (West 2008). At its passage, the statute stirred significant controversy given its inclusion of the term “annoy” because the term might capture a wide range of anonymous Internet banter that falls short of cyber stalking. Goodno, *supra* note 236, at 149; Posting of Daniel J. Solove to Concurring Opinions, http://www.concurringopinions.com/archives/2006/01/annoy_someone_o.html#c1603 (Jan. 10, 2006, 00:27). Courts have responded to this controversy, finding that although the statute might have unconstitutional applications, it would not warrant facial invalidation on vagueness or over breadth grounds. *See, e.g.*, *United States v. Eckhardt*, 466 F.3d 938, 943-44 (11th Cir. 2006).

that are transmitted, in whole or in part, by the Internet.”²⁴⁹ The provision applies to individuals who anonymously and intentionally harass or threaten another over the Internet.²⁵⁰ Given prosecutors’ reluctance to date to invoke VAWA,²⁵¹ Congress would do well to enact a parallel civil remedy to accompany it, much as § 1985(3) and § 1986 supplement § 241.

III. PROTECTING ONLINE DIALOGUE

Civil rights movements have fairly similar life cycles. In its first stage, the movement seeks recognition of a marginalized group’s members as social equals worthy of respect. At this stage, the law has an enormous impact on the well-being of subordinated people – such as its recognition of equal citizenship, the ability to marry, the right to own property, and so forth – but only a minor impact on society’s overall functionality.²⁵² Here, the movement can be characterized primarily as an assault on the most gratuitous manifestations of discrimination.

Bringing full equality to formerly subordinated people, however, typically requires more. The civil rights movement next comes into conflict with entrenched societal values. Abolitionists faced claims of property rights and states’ rights.²⁵³ The civil rights movement of the mid-twentieth century again confronted claims for limited government and states’ rights.²⁵⁴ More recent efforts to integrate people of color, and women, into public life have faced similar resistance, asserting New Deal norms of efficiency and merit.²⁵⁵ In each case, advocates of the entrenched, supposedly neutral norm insist that it must be upheld absolutely lest the law slide down a slippery slope leading to a profoundly worse society.²⁵⁶ Implicit, and sometimes explicit, in these calls to

²⁴⁹ 47 U.S.C.A. § 223(h)(1)(C).

²⁵⁰ *United States v. Tobin*, 545 F. Supp. 2d 189, 193 (D.N.H. 2008) (finding that a defendant must “have a specific purpose to cause emotional upset in a person”). Naomi Goodno suggests that cyberstalking statutes may be inapplicable to online postings that terrorize victims and may only apply to e-mail directed to the victim. Goodno, *supra* note 236, at 149. Yet VAWA extends to communications “originat[ing]” from a “device or software” that were “transmitted, in whole or in part, by the Internet” to a victim who “receives the communication,” 47 U.S.C.A. § 223(a)(1)(C)-(h)(1)(C), and thus a less restrictive reading is certainly possible.

²⁵¹ Kelli C. McTaggart, Note, *The Violence Against Women Act: Recognizing a Federal Civil Right to Be Free from Violence*, 86 GEO. L.J. 1123, 1146 (1998).

²⁵² BERNARD SCHWARTZ, *THE LAW IN AMERICA: A HISTORY* 94 (1974).

²⁵³ See Austin Allen, *Rethinking Dred Scott: New Context for an Old Case*, 82 CHL.-KENT L. REV. 141, 145 (2007).

²⁵⁴ See FRIEDMAN, *supra* note 3, at 526. Absolutist claims based on these norms successfully derailed the Reconstruction-era civil rights movement, leading to a century of brutal subordination and hardship that discredited rather than strengthening states’ rights.

²⁵⁵ See LAWRENCE M. FRIEDMAN, *LAW IN AMERICA: A SHORT HISTORY* 143 (2002).

²⁵⁶ See, e.g., David E. Bernstein, *Defending the First Amendment from Antidiscrimination Laws*, 82 N.C. L. REV. 223, 227-28 (2003) (arguing that

hold supposedly neutral norms inviolate is a demand that marginalized individuals sacrifice full equality for the greater good.²⁵⁷

In hindsight, these absolutists appear misguided. Requiring foundational norms to accommodate civil rights did not destroy those norms but, in some cases, strengthened them. Property rights had never been absolute, and ceasing to treat human beings as the property of another buttressed property law's credibility by separating it from the ignominy of slavery. States and public accommodations lost the right to exclude or discriminate on the basis of race, yet states' powers have, if anything, grown, perhaps because states seem more trustworthy having shed the baggage of Jim Crow. Civil rights legislation did not stop deregulation and deep tax cuts from shrinking government. And as employers come to grips with the realities of diverse workplaces and accommodation of people with disabilities, they are finding that diverse environments do not sacrifice efficiency, but, in fact, enhance it.²⁵⁸

If past conflicts between civil rights and those foundational values seem contrived today, it is because we recognize that those values retain their power without being absolute²⁵⁹ and that accommodating them to civil rights norms has not led to their wholesale collapse. We should assess the argument that free speech absolutism should trump civil rights concerns in light of this history.

In much the same way the pre-Industrial Age underscored the importance of property rights and the Industrial Age exalted private ordering through contract, the Information Age depends upon the Internet for its economic success. The Internet is also as fundamental to shaping our current political order as the concepts of states' rights and limited government were in an earlier age.²⁶⁰ Just as changing circumstances justified curtailing the right to contract in the 1930s, today's networked environment warrants a rejection of free-speech absolutism.²⁶¹ Allowing women, people of color, and other

antidiscrimination laws threaten free speech and that the government's weakening of civil liberties in favor of equality threatens to undermine all other liberties).

²⁵⁷ See J.M. Balkin, *Some Realism About Pluralism: Legal Realist Approaches to the First Amendment*, 1990 DUKE L.J. 375, 383-84 [hereinafter Balkin, *Realism About Pluralism*] (explaining that the Ku Klux Klan embraced an absolutist approach to the First Amendment that once held sway with civil rights activists of the 1950s and 1960s in denouncing laws that combat racial discrimination).

²⁵⁸ See *id.* at 420-21 (arguing that an absolutist approach to the First Amendment is misguided when addressing sexual and racial harassment in the workplace as there will be no counter speech due to the directness of the intimidation).

²⁵⁹ See RONALD DWORKIN, *TAKING RIGHTS SERIOUSLY* 92 (1977) (contrasting absolute and less-than-absolute rights and noting that the strength of society's commitment to a particular right can be assessed by which other rights society allows that particular right to trump).

²⁶⁰ YOCHAI BENKLER, *THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM* 232 (2006).

²⁶¹ Balkin, *Realism About Pluralism*, *supra* note 257, at 383.

vulnerable people to be denied the full panoply of the opportunities available on the Internet, rather than searching for a meaningful accommodation with other important norms, would constitute a heavy blow to both civil rights and civil liberties.

Section A argues that robust protection of civil rights on the Internet would, in fact, promote far more valuable speech than it would inhibit. Section B looks more broadly at normative bases of the protection of free speech in society, finding that a balancing of civil rights goals with free speech values is feasible and desirable here. Section C explores why First Amendment doctrine does not impede the protections of cyber civil rights described in Part II.

A. *Online Mobs and Individual Autonomy*

One of free speech's most important functions is promoting individual autonomy.²⁶² This view urges that people be free to choose their own path.²⁶³ Free speech facilitates self-mastery, allowing people to author their own narratives.²⁶⁴ Commentators characterize respect for autonomy of speech and thought as necessary for legitimate government.²⁶⁵ For some, freedom from any form of coercion is paramount for autonomy and dignity.²⁶⁶ Others argue that autonomy and dignity require equitable and effective participation in political self-government, and thus the regulation of certain speech, such as racist and sexist speech, may be an essential prerequisite to secure equal citizenship.²⁶⁷

Restraining a mob's most destructive assaults is essential to defending the expressive autonomy and equality of its victims.²⁶⁸ Preventing mobs from driving vulnerable people offline would "advance the reasons why we protect free speech in the first place," even though it would inevitably chill some

²⁶² See, e.g., THOMAS I. EMERSON, *THE SYSTEM OF FREEDOM OF EXPRESSION* 6-7 (1970); C. Edwin Baker, *Scope of the First Amendment Freedom of Speech*, 25 *UCLA L. REV.* 964, 964-66 (1978); Richard H. Fallon, Jr., *Essay, Two Senses of Autonomy*, 46 *STAN. L. REV.* 875, 875 (1994); Martin H. Redish, *The Value of Free Speech*, 130 *U. PA. L. REV.* 591, 593 (1982) ("[F]ree speech ultimately serves only one true value, which I have labeled 'individual self-realization.'").

²⁶³ RONALD DWORIN, *A MATTER OF PRINCIPLE* 61 (1985); Redish, *supra* note 262, at 593.

²⁶⁴ JOSEPH RAZ, *THE MORALITY OF FREEDOM* 408-10 (1986).

²⁶⁵ Robert C. Post, *Racist Speech, Democracy, and the First Amendment*, 32 *WM. & MARY L. REV.* 267, 279-85 (1991).

²⁶⁶ *Id.* at 284; see EMERSON, *supra* note 262, at 6.

²⁶⁷ See Mary Ellen Gale, *Reimagining the First Amendment: Racist Speech and Equal Liberty*, 65 *ST. JOHN'S L. REV.* 119, 155-56 (1991) (arguing that positive freedom requires "recognition and respect as an equal, autonomous self" and "protection or release from nongovernmental social constraints"); Frank Michelman, *Law's Republic*, 97 *YALE L.J.* 1493, 1531-32 (1988).

²⁶⁸ See FISS, *supra* note 153, at 15.

speech of online mobs.²⁶⁹ Free from mob attacks, victims might continue to blog, join online discussions, and generally express themselves on public issues. Protecting them from grotesque defamation, threats, invasions of privacy, and technological attacks would allow them to be candid about their ideas.²⁷⁰

Although online mobs express themselves and their autonomy through their assaults, their actions also implicate their victims' autonomy and ability to participate in political and social discourse.²⁷¹ Self-expression should receive no protection if its sole purpose is to extinguish the self-expression of another.²⁷² As Owen Fiss argues, sometimes we must lower the voices of some to permit the self-expression of others.²⁷³ Similarly, Cass Sunstein contends that threats, libel, and sexual and racial harassment constitute low-value speech of little First Amendment consequence.²⁷⁴ Rarely is that more true than when one group of voices consciously exploits the Internet's aggregating power to silence others and its disaggregative power to escape social responsibility for the group's actions.

B. *Civil Rights and the Theory of Free Speech Online*

The importance of free speech warrants vigilance against threats that weaken public discourse.²⁷⁵ These concerns, however, are not absolute.²⁷⁶ Our society permits restrictions on speech that is "of such slight social value as a step to truth that any benefit that may be derived from [it] is clearly outweighed by the social interest in order and morality."²⁷⁷ The Internet poses several challenges to striking that balance.

This Section explores the challenges of applying First Amendment theory to cyberspace. Section 1 identifies the special problem of distinguishing

²⁶⁹ See SOLOVE, *supra* note 4, at 129.

²⁷⁰ *Id.* at 131.

²⁷¹ See FISS, *supra* note 153, at 16 (arguing that hate speech regulations address speech that vitiates a disadvantaged group's ability to contribute to public discussion).

²⁷² STEVEN J. HEYMAN, *FREE SPEECH, HUMAN DIGNITY* 166 (2008).

²⁷³ See FISS, *supra* note 4, at 18; Owen M. Fiss, *Why the State?*, 100 HARV. L. REV. 781, 786 (1987) ("Autonomy may be protected, but only when it enriches public debate."); accord CASS R. SUNSTEIN, *DEMOCRACY AND THE PROBLEM OF FREE SPEECH* 127 (1995).

²⁷⁴ SUNSTEIN, *supra* note 273, at 11.

²⁷⁵ Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. (forthcoming 2008); see Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect,"* 58 B.U. L. REV. 685, 689 (1978). A host of theories offer competing explanations of the First Amendment. See Richards, *supra*. This Article does not discuss the merits of these theories in the abstract but instead addresses those that present the most compelling arguments against challenging online mobs.

²⁷⁶ SOLOVE, *supra* note 4, at 128-29; T. Alexander Aleinikoff, *Constitutional Law in the Age of Balancing*, 96 YALE L.J. 943, 947 (1987).

²⁷⁷ *Chaplinsky v. New Hampshire*, 315 U.S. 568, 572 (1942).

protected expressions from unprotected actions in a medium that functions exclusively by transmitting packets of data. Section 2 considers online mobs in the context of some prominent First Amendment theories. Section 3 assesses whether private correction of online mobs' abuses might obviate the need for a legal response. Finally, Section 4 explores the extent to which online mobs' protected speech might be curtailed or chilled by enforcement of the doctrines advocated here.

1. The Expression-Action Distinction on the Internet

A core problem in theorizing the First Amendment is distinguishing expressions from actions. This speech-conduct dichotomy pervades free speech discourse.²⁷⁸ Advances in law and technology, however, complicate this distinction as they make more actions achievable through "mere" words. Indeed, the Internet's very essence is to aggregate expressions so as to convert them into actions. Some Internet behaviors that are akin to the offline crimes of breaking and entering and vandalism – hacking and denial-of-service attacks – are accomplished by sending communications to other computers. Moreover, the Internet's powerful aggregative capacity converts seemingly individual expressions (e.g., visiting a website or sending an e-mail) into criminal acts through their repetition (e.g., denial-of-service attacks and image reaping). The Internet also routinely allows individuals to aggregate their efforts with strangers. Thus, the fact that someone may not know the identity of a thief or rapist who uses posted personal information does not eliminate the danger, because the poster knows that such predators may put the information to malicious use.

The Internet may also disaggregate communications into components that operate as actions. For example, some online rape threats engender serious fear that they will be carried out offline because they arrive without cues – such as the identity or location of the person who made the threat or a joking tone of voice – that might diminish the nature of the threat.²⁷⁹ The person's refusal to leave cues that would mitigate the victim's fear arguably demonstrates that person's intent to terrorize the victim. This can convert expression into criminal conduct. In short, because everything that happens on

²⁷⁸ EMERSON, *supra* note 262, at 8, 17 (explaining that the theory of expression rests upon a "fundamental distinction" between expression and action, which permits society to exercise more control over action than expression if the action is not controlled by limiting expression, because freedom of expression is essential to personality and all other freedoms and because expression does less injury to other social goals than action and has less immediate consequences).

²⁷⁹ THE SOCIAL NET: UNDERSTANDING HUMAN BEHAVIOR IN CYBERSPACE 248 (Yair Amichai-Hamburger ed., 2005); Shaheen Shariff & Leanne Johnny, *Cyber-Libel and Cyber-Bullying: Can Schools Protect Student Reputations and Free-Expression in Virtual Environments?*, 16 EDUC. & L.J. 307, 314 (2007).

the Internet ultimately takes the form of 1s and 0s does not mean that it is all the expression of ideas.

The expression-action distinction for cyberspace is elusive.²⁸⁰ One could argue that hacking and denial-of-service attacks work first on computers and only indirectly on the computers' owners. The same, however, could be said of responding to an online poll or visiting a site solely to enhance its hit count. Alternatively, one could categorize online activity based on its offline analogues. Unfortunately, this would lead to difficult debates over the strength of competing analogies. Even more importantly, this approach ignores the ways in which the Internet's aggregative and disaggregative character fundamentally transforms online activity. One might ask which characteristic – expression or action – dominates the activity.²⁸¹ But this question may be difficult to answer, as behavior is often equal parts expression and action.²⁸² For instance, the picture with Ms. Sierra being suffocated by lingerie²⁸³ arguably constitutes both action meant to terrorize her and expression designed to communicate feelings of hatred and misogyny.

A final option would be to treat online behavior as conduct if a reasonable person would expect or intend it to have offline effects independent of the expression of ideas. Thus, threats that frighten recipients and disclosures of personal information that empower identity thieves to obtain victims' money could both be regarded as criminal conduct, like denial-of-service attacks and hacking. This principle would compel some judgment calls, although these would be broadly similar to those the Court's Confrontation Clause doctrine requires in determining the admissibility of statements of witnesses who are unavailable for cross-examination.²⁸⁴ It would, however, take full account of the fundamental changes in our modes of both expression and action wrought by the Internet.

²⁸⁰ Indeed, as Fred Lawrence persuasively explains, the action-expression distinction is elusive no matter the context. Frederick M. Lawrence, *Resolving the Hate Crimes/Hate Speech Paradox: Punishing Bias Crimes and Protecting Racist Speech*, 68 NOTRE DAME L. REV. 673, 692-93 (1993) [hereinafter Lawrence, *Resolving Paradox*]. This argument has even more force in cyberspace given the aggregative and disaggregative qualities of online activity.

²⁸¹ See EMERSON, *supra* note 262, at 18.

²⁸² John Hart Ely, Comment, *Flag Desecration: A Case Study in the Roles of Categorization and Balancing in First Amendment Analysis*, 88 HARV. L. REV. 1482, 1495-96 (1975); Lawrence, *supra* note 280, at 692-94 (explaining, for example, that burning a cross on the lawn of an African-American family is "one hundred percent action directed against" the family and "one hundred percent expression of deeply-felt racism").

²⁸³ See *supra* note 18 and accompanying text.

²⁸⁴ See *Crawford v. Washington*, 541 U.S. 36, 59 (2004).

2. The Values the First Amendment Protects

Freedom of expression serves several important purposes.²⁸⁵ Limiting online mobs' abuses as proposed above would not threaten any of their core values. Freedom of expression facilitates deliberation about public issues and hence promotes democratic governance.²⁸⁶ Under this view, expression deserves protection if it promotes ideas and information necessary for a self-governing citizenry to make decisions about what kind of life it wishes to live.²⁸⁷ A mob's online attacks do not involve discourse on political issues. Quite the contrary, the attacks deprive vulnerable individuals of their right to engage in political discourse. The threats, lies, and damaging photographs generate a fear of physical violence, exclusion, and subordination that may propel victims offline.²⁸⁸

Democratic culture theorists argue that freedom of expression promotes "democracy in the widest possible sense, not merely at the level of governance, or at the level of deliberation, but at the level of culture" where we interact, create, build communities, and build ourselves.²⁸⁹ Free speech permits innovation in a networked age where people aggregate their ideas with those of others, create works of art, gossip, and parody, and thus continually add to the cultural mix in which they live.²⁹⁰ It enables individuals to participate in creating culture on equal terms.²⁹¹ Free speech also dissolves unjust social barriers of rank and privilege.²⁹² In this vein, Diane Zimmerman highlights the role of gossip as generating intimacy and a sense of community among disparate groups.²⁹³ Gossip provides people a way to learn about social groups

²⁸⁵ See, e.g., EMERSON, *supra* note 262, at 6-7; LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW 785-89 (2d ed. 1988) (emphasizing two values protected by the First Amendment – the intrinsic value of speech, which is the value of self-expression, and the instrumental value of speech – and how the First Amendment protects dissent to maximize public discourse, to achieve robust debate and ideas, and to make our democracy work).

²⁸⁶ TRIBE, *supra* note 285, at 577; Alexander Meiklejohn, *The First Amendment Is an Absolute*, 1961 SUP. CT. REV. 245, 255.

²⁸⁷ ALEXANDER MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT 25-27 (1948); Robert H. Bork, *Neutral Principles and Some First Amendment Problems*, 47 IND. L.J. 1, 26 (1971); Owen M. Fiss, Essay, *Free Speech and Social Structure*, 71 IOWA L. REV. 1405, 1409-10 (1986).

²⁸⁸ See SUNSTEIN, *supra* note 273, at 186 (arguing that hate speech such as the word "ni[**]er" creates fears of physical violence, exclusion, and subordination that silence individuals).

²⁸⁹ Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 34 (2004).

²⁹⁰ *Id.*

²⁹¹ *Id.* at 35.

²⁹² *Id.*

²⁹³ Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 333-34 (1983).

to which they do not belong and fosters relationships by giving strangers the means to bridge awkward silences when thrown together in social situations.²⁹⁴

Online mobs do indeed engage in gossip. Sites such as JuicyCampus promote themselves as gossip facilitators. But the attacks perpetrated by online mobs have little to do with building bonds among disparate communities. Rape threats, lies, damaging photographs, and denial-of-service attacks not only preclude any connection with differently-minded group members, but they also sever the victim's connections with her own community. The attacks inflict serious social harm rather than generating ideas in popular culture or enforcing positive social norms. Defeating such discrimination outweighs the imperceptible contribution that online mobs make to our cultural interaction and exchange.

Still others focus on free speech as an engine promoting truth.²⁹⁵ In this view, any silencing of speech prevents us from better understanding the world in which we live.²⁹⁶ Justice Holmes drew from this theory when he articulated the notion of the marketplace of ideas: "that the best test of truth is the power of the thought to get itself accepted in the competition of the market."²⁹⁷ The marketplace-of-ideas metaphor places no special premium on political discussion.²⁹⁸ Instead, it captures the idea that "truth must be experimentally determined from the properties of the experience itself."²⁹⁹

An extreme version of truth-seeking theory might insist the market should sort out online mobs' deceptions. Though to do so, the theory would have to consider a Social Security number a truthful fact, disclosure of which contributes to an understanding of that person.³⁰⁰ A more plausible vision of truth-seeking theory, however, is not served with the disclosure of a person's

²⁹⁴ *Id.* at 334; see also Robert Post, *The Legal Regulation of Gossip: Backyard Chatter and the Mass Media*, in GOOD GOSSIP 65, 65 (Robert F. Goodman & Aaron Ben-Ze'ev eds., 1994).

²⁹⁵ ISIAH BERLIN, *Two Concepts of Liberty*, in FOUR ESSAYS ON LIBERTY 118, 128 (1969); Frederick F. Schauer, *Language, Truth, and the First Amendment: An Essay in Memory of Harry Canter*, 64 VA. L. REV. 263, 272 (1978) (describing the marketplace of ideas theory where the views and speech accepted by those in the marketplace are "true" and the views and speech rejected by the marketplace are "false.").

²⁹⁶ Robert Post, *Reconciling Theory and Doctrine in First Amendment Jurisprudence*, 88 CAL. L. REV. 2353, 2363 (2000).

²⁹⁷ *Abrams v. United States*, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting); see also *Red Lion Broad. Co. v. FCC*, 395 U.S. 367, 390 (1969) ("It is the purpose of the First Amendment to preserve an uninhibited marketplace of ideas in which truth will ultimately prevail" (citations omitted)).

²⁹⁸ SUNSTEIN, *supra* note 273, at 25.

²⁹⁹ Post, *supra* note 296, at 2360.

³⁰⁰ See RICHARD A. POSNER, *THE ECONOMICS OF JUSTICE* 232-38 (1981) (seeing personal information's main purpose as allowing the market to judge an individual).

personal identifying information.³⁰¹ Rather than revealing a fact to be tested in the marketplace, a Social Security number is simply a key to a person's credit and bank accounts.³⁰² In this context, it is a weapon, not a truth or half-truth to be tested in the marketplace. Rape and death threats similarly tell us nothing about the victims – no truths are contested there. This is equally true of denial-of-service attacks and “image reaping.” Even where online mobs make factual assertions, features of the Internet prevent the marketplace of ideas from performing its intended curative function, as the next Section shows. Moreover, as Daniel Solove notes, “truth isn't the only value at stake.”³⁰³

3. The Inadequacy of Private Responses

One common offline response to some kinds of unpleasant speech is exclusion of the speaker. Someone who disrupts a private party or meeting may not receive an invitation back. A proliferation of annoying sound trucks may yield time, place, and manner restrictions, such as a noise ordinance.³⁰⁴ Stations that broadcast obscenity when children often listen may lose their licenses.³⁰⁵ Although exclusion can be ineffective against many forms of offensive expression offline, it is particularly ineffective online where individuals can easily frustrate any exclusion by disaggregating their on- and offline identities: an individual ejected from a website under one screen name could promptly return under another.

Nonetheless, some may argue that private responses obviate the need for criminal, tort, and civil rights remedies. In particular, they may contend that victims can defeat online crowds without this proposal by recruiting advocacy

³⁰¹ The release of sensitive information, such as a person's medical condition, may not advance the truth-seeking function of the marketplace. Cognitive and behavioral psychologists, sociologists, and economists challenge the notion that people with access to information will use it to make rational decisions. ARCHON FUNG, MARY GRAHAM & DAVID WEIL, *FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY* 33 (2007). Individuals are prone to cognitive distortions that may lead them to make decisions that differ from those predicted in a world of perfect rationality. Paul Horwitz, *Free Speech as Risk Analysis: Heuristics, Biases, and Institutions in the First Amendment*, 76 *TEMP. L. REV.* 1, 6 (2003). This argument may be particularly persuasive where information confirms discriminatory biases. See C. Edwin Baker, *Scope of the First Amendment Freedom of Speech*, 25 *UCLA L. REV.* 964, 976 (1978); Jerome A. Barron, *Access to the Press – A New First Amendment Right*, 80 *HARV. L. REV.* 1641, 1678 (1967).

³⁰² See Citron, *supra* note 43, at 252-53.

³⁰³ SOLOVE, *supra* note 4, at 132.

³⁰⁴ See *Cohen v. California*, 403 U.S. 15, 21 (1971) (holding a jacket with the phrase “F[**]k the Draft” on the back worn in a courthouse was protected speech because “persons confronted with [the] jacket were in a quite different posture than, say, those subjected to the raucous emissions of sound trucks blaring outside their residences”).

³⁰⁵ See *FCC v. Pacifica Found.*, 438 U.S. 726, 738 (1978) (finding the FCC was warranted in sanctioning licensees who engage in obscene, indecent, or profane broadcasting).

groups to defend them. Women's groups could coordinate efforts to rebuild a victim's reputation online. They could engage in "Google-bombing" to optimize positive posts on a search of a victim's name. Groups like ReputationDefender have helped victims establish their online presence to offset destructive postings.³⁰⁶

Such a response, however, would be inadequate. First, it would not remove the threats and lies that produce emotional distress and fear. It would not restore the confidentiality of the victim's Social Security number and other sensitive information. Even in the case of "merely" defamatory attacks, it is inconceivable that all damage will be restored.³⁰⁷ Because so many people will see the material, some will inevitably miss the victim's response while others will not believe, or only partially believe, it. In the diffuse world online, the shortcomings of any response will be much, much worse.

When issues are being debated, the failure of a point to connect with its counterpoint is less of a concern: some people's views may be skewed by seeing only one side of an argument, while others' ideas may reflect disproportionate exposure to the opposing side. In the end, society can hope the two roughly balance. When dealing with attacks on someone's character, however, the victim does not have an affirmative case she is trying to convey – she is only seeking to dispel the harm from the mob's attack. People seeing a disproportionate number of her rebuttals will not counterbalance those who have seen none.

Second, the efforts of advocacy groups may be unable to drown out the assaults of cyber mobs. Consider the case of Nicole Catsouras, who died in a horrific car crash.³⁰⁸ Gruesome photographs of the carnage appeared on the Internet, spreading to over 1500 sites.³⁰⁹ Posters urged cohorts to harass her family and facilitated this harassment by providing the family's home address.³¹⁰ The woman's family asked sites to remove the pictures but to no avail.³¹¹ Tracking down the anonymous posters proved impossible for the family, and the pictures remained online.³¹²

Third, instead of slowing down an online mob, counter-measures may sustain the life of the attacks. The very purpose of many online attacks is to force victims off the net; the mobs are likely to respond with particular venom against a victim who not only stays online but tries to fight back. A victim may plausibly conclude that more people will see the defamatory or private material if she responds than if she does not.

³⁰⁶ See *supra* note 87 and accompanying text.

³⁰⁷ Cohen, *supra* note 207, at 245.

³⁰⁸ Victoria Murphy Barret, *Anonymity & the Net*, FORBES, Oct. 15, 2007, at 74.

³⁰⁹ *Id.*

³¹⁰ *Id.*

³¹¹ *Id.*

³¹² *Id.*

Fourth, online attacks are vastly more numerous and easier to launch than defenses. The online advocacy groups are hopelessly outnumbered and outmatched, and basic collective action theory says they will remain so.³¹³ Few free or inexpensive resources are available for defending one's online reputation, and the services of groups like ReputationDefender are expensive and beyond the means of many victims.³¹⁴ Even if a victim could afford such assistance, anticipating that cost could discourage an individual from expressing herself online. Thus, the fact that *some* victims of mobs may be able to enlist allies does not justify limiting or denying relief to the many who cannot.

Finally, this view ignores the social harm resulting from attacks by online mobs. If expressing opinions online subjects someone to the risk of assault, even if the damage is only temporary, the result will change the kinds of people who participate in online discourse. If we believe the Internet is, and should remain, a wild west with incivility and brutality as the norm, then those who are impervious to such conduct will remain online while the vulnerable may not. To that end, we may get more bull-headed posters and fewer thoughtful ones. An online discourse which systematically under-represents people – particularly women and people of color – cannot effectively process our various attitudes and convert them into truly democratic decisions.

4. The Extent of Interference with Protected Expression

In considering restrictions on the time, place, and manner of expression, the Supreme Court has emphasized the availability of alternative avenues for expression.³¹⁵ Although defamation, true threats, and online mobs' other unlawful actions are subject to far more extensive regulation than merely time, place, and manner, this reasoning is nonetheless instructive. None of the criminal statutes, tort laws, and civil rights theories discussed here impede or even chill the mobs' expression of their core ideas, whether they be disagreement with their targets' ideas, hatred for their targets, or even hatred of women or other classes of people. In addition, no statutes limit the vehemence of those expressions. They instead further important interests unrelated to the suppression of hateful, racist, or sexist speech.

Although the Court has upheld excluding from public property fully protected expressions of political and religious views in ways that sharply

³¹³ See Robert L. Glicksman & Richard E. Levy, *A Collective Action Perspective on Ceiling Preemption by Federal Environmental Regulation: The Case of Global Climate Change*, 102 NW. U. L. REV. 579, 579 n.1 (2008) (explaining collective action theory as one that examines the dynamics of individual behavior in cooperative group settings and concludes that individual members of a collective group usually do not act because they have the incentive to "free ride" on the efforts of others).

³¹⁴ See, e.g., ReputationDefender: Frequently Asked Questions, <http://www.reputationdefender.com/faq> (last visited Nov. 5, 2008).

³¹⁵ *Frisby v. Schultz*, 487 U.S. 474, 482 (1988).

narrowed their potential audiences,³¹⁶ none of the remedies proposed here would curtail in any way the audience for the mobs' expressions of disagreement. At the margins, of course, some may be uncertain as to whether a particular threat will be considered sufficiently severe to qualify as a true threat or whether particular abuse is sufficiently outrageous to be considered an intentional infliction of emotional distress. These problems, however, existed in the analog world, and they affect only a tiny fraction of the ways in which an idea might be expressed. Protecting the civil rights of online mobs' victims comes at an extremely small cost to legitimate expression.

C. *First Amendment Doctrine*

1. Criminal and Tort Law

Threats fall outside the First Amendment's protection if speakers mean to communicate a serious intention to commit an act of unlawful violence against particular individuals.³¹⁷ The speaker need not actually intend to commit a violent act because the prohibition of "true threats" protects individuals from the fear of violence and the disruption that such fear engenders.³¹⁸ Once a statement meets the "true threat" standard, it no longer qualifies as protected speech because it "is so intertwined with violent action that it has essentially become conduct."³¹⁹

A "true threat" determination typically depends upon whether a reasonable person would consider the statement a serious and unconditional expression of intent to inflict bodily harm and not mere hyperbole.³²⁰ A person, however, cannot escape responsibility merely by combining the threatening language

³¹⁶ See, e.g., *Int'l Soc'y for Krishna Consciousness, Inc. v. Lee*, 505 U.S. 672, 685 (1992) (upholding a ban on solicitations in publicly operated airport terminals).

³¹⁷ *Virginia v. Black*, 538 U.S. 343, 359 (2003); *R.A.V. v. City of St. Paul*, 505 U.S. 377, 388 (1992) (explaining that threats fall outside the First Amendment to "protect[] individuals from the fear of violence, from the disruption that fear engenders, and from the possibility that the threatened violence will occur"); *Watts v. United States*, 394 U.S. 705, 708 (1969).

³¹⁸ *Black*, 538 U.S. at 359-60.

³¹⁹ *United States v. Francis*, 164 F.3d 120, 123 (2d Cir. 1999) (citation omitted).

³²⁰ *Watts*, 394 U.S. at 705-08 (deeming the statement, "[i]f they ever make me carry a rifle the first man I want to get in my sights is L.B.J." political hyperbole, a "kind of very crude offensive method of stating political opposition to the President," and not a true threat because it was made at a protest rally, it had an expressly conditional nature, and it prompted listeners to laugh). Only the Ninth Circuit requires proof that the defendant subjectively intended to threaten the victim. *United States v. Twine*, 853 F.2d 676, 680 (9th Cir. 1988). The remaining circuits apply an objective standard that focuses on whether it was reasonably foreseeable to the speaker (or the listener) that the statement would be interpreted as expressing a serious intent to hurt another. E.g., *United States v. Syring*, 522 F. Supp. 2d 125, 129 (D.D.C. 2007).

with an issue of public concern.³²¹ Courts have upheld online threats as unprotected “true threats” even though the defendants never sent the messages directly to the recipients.³²² Whether statements constitute “true threats” is a jury question unless no reasonable jury could find that they amounted to “true threats.”³²³

Similarly, First Amendment doctrine offers little protection to defamatory statements because they offer “such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality.”³²⁴ Statements do, however, enjoy immunity from defamation liability if they do not assert or imply verifiable facts.³²⁵ To

³²¹ Frederick M. Lawrence, *The Collision of Rights in Violence-Conducive Speech*, 19 CARDOZO L. REV. 1333, 1355-56 (1998); *see, e.g.*, *Planned Parenthood of Columbia/Willamette, Inc. v. Am. Coal. of Life Activists*, 290 F.3d 1058, 1079-80, 1085 (9th Cir. 2002) (en banc) (holding that “Wanted” posters and a portion of the Nuremberg Files website that listed abortion doctors’ home and work addresses went “well beyond the political message” that “abortionists are killers who deserve death” and were true threats because even though the posters and website contained no explicitly threatening language, they connotated the message “You’re Wanted or You’re Guilty; You’ll be shot or killed” in light of the prior murders of physicians who appeared on Wanted posters); *United States v. Bellrichard*, 994 F.2d 1318, 1322 (8th Cir. 1993); *United States v. Khorrami*, 895 F.2d 1186, 1192-94 (7th Cir. 1990) (upholding a conviction where a defendant sent a “Wanted” poster with pictures of Israeli officials to the Jewish National Fund headquarters); *Syring*, 522 F. Supp. 2d at 126, 131 (refusing to dismiss a 18 U.S.C § 875(c) (2000) indictment because it was a fact question for the jury, where a defendant sent e-mails and voicemails to a victim’s workplace that said “[named individual’s] anti-American statements . . . are abhorrent The only good Lebanese is a dead Lebanese”).

³²² *See, e.g.*, *United States v. Sutcliffe*, 505 F.3d 944, 952-53 (9th Cir. 2007) (upholding a § 875(c) conviction where a defendant posted a threat on his website to kill a company’s process server and uploaded a picture of the company’s attorney and her daughter, along with her home address, while a voiceover clip played from a movie that featured the stalking of an attorney and his family); *United States v. Morales*, 272 F.3d 284, 288 (5th Cir. 2001) (affirming a § 875(c) conviction where the defendant sent instant messages under the name Ed Harris to a third party unconnected to the defendant’s high school stating that he “will kill” teachers and students at his school, because the defendant repeated his threats several times, gave no indication that he was joking, and admitted that he attempted to refer to Columbine High School killer Eric Harris).

³²³ *See, e.g.*, *United States v. Zavalidroga*, No. 97-10290, 1998 WL 403361, at *1 (9th Cir. July 7, 1998); *United States v. Whiffen*, 121 F.3d 18, 22 (1st Cir. 1997).

³²⁴ *Chaplinsky v. New Hampshire*, 315 U.S. 568, 572 (1942); *see, e.g.*, *Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 245-46 (2002) (explaining that “freedom of speech has its limits” and “does not embrace certain categories of speech, including defamation”); *Beauharnais v. Illinois*, 343 U.S. 250, 266 (1952).

³²⁵ *Milkovich v. Lorain Journal Co.*, 497 U.S. 1, 18-20 (1990). The Supreme Court explained: “If a speaker says, ‘In my opinion, John Jones is a liar,’ he implies a knowledge of facts which lead to the conclusion that Jones told an untruth,” and the comment can be actionable. *Id.* at 18. By contrast, if the speaker says a person “shows his abysmal ignorance by accepting the teachings of Marx and Lenin,” the First Amendment bars

that end, courts prohibit defamation actions based on loose, figurative language that no reasonable person in that context would believe presented facts.³²⁶ For example, criticizing another's views in an online debate has been understood as constituting privileged opinion and not verifiable facts.³²⁷

Nonetheless, anonymous message-board postings are not immune from defamation liability simply because they are too outrageous to be believed.³²⁸ A California court explained:

Even if the exchange that takes place on these message boards is typically freewheeling and irreverent, we do not agree that it is exempt from established legal and social norms. . . . We would be doing a great disservice to the Internet audience if we were to conclude that all speech on Internet bulletin boards was so suspect that it could not be defamatory as a matter of law.³²⁹

If these damaging statements here were indeed false, many would not enjoy immunity from liability – they could reasonably be understood as asserting verifiable facts. For instance, statements concerning a victim's specific actions or conditions, such as a stay in a drug rehabilitation center, an infectious disease, or a specific LSAT score, seem factual, and thus, a plaintiff could prove them true or false for defamation purposes.³³⁰

recovery because the statement cannot be objectively verified. *Id.* at 20. For example, calling a play a “rip-off, a fraud, a scandal, a snake-oil job” constituted hyperbole that deserved constitutional protection. *Phantom Touring, Inc. v. Affiliated Publ'ns*, 953 F.2d 724, 728 (1st Cir. 1992).

³²⁶ *See, e.g.*, *Old Dominion Branch No. 496, Nat'l Ass'n of Letter Carriers v. Austin*, 418 U.S. 264, 284-86 (1974) (holding that the use of the word “traitor” to define a worker who crossed a picket line was not actionable).

³²⁷ *See, e.g.*, *Nicosia v. De Rooy*, 72 F. Supp. 2d 1093, 1101 (N.D. Cal. 1999) (finding that an online debate between parties in a legal dispute did not constitute verifiable facts because the audience would anticipate efforts by the parties to persuade others of their position through fiery epithets and hyperbole); *Krinsky v. Doe 6*, 72 Cal. Rptr. 3d 231, 248-50 (Ct. App. 2008) (finding statements in a defamation suit not actionable where the defendant posted statements accusing the plaintiff of having a “fake medical degree” and being a “crook” with “poor feminine hygiene” because the statements were part of a “[h]eated discussion” between the parties on an online message board).

³²⁸ *See, e.g.*, *Varian Med. Sys., Inc. v. Delfino*, 6 Cal. Rptr. 3d 325, 337 (Ct. App. 2003) (rejecting defendant's argument that his online statements calling the plaintiffs liars who suffered from mental illnesses and had sex with their employers were opinions or hyperbole because “no reasonable person would take a typical anonymous and outrageous posting as a true statement of fact”), *rev'd on other grounds*, 106 P.3d 958 (Cal. 2005); *Super Future Equities, Inc. v. Wells Fargo Bank*, 553 F. Supp. 2d 680, 688 (N.D. Tex. 2008) (refusing to consider online statements that accused the plaintiff of engaging in particular conduct as protected opinions because they could be understood as verifiable facts).

³²⁹ *Varian*, 6 Cal. Rptr. 3d at 337.

³³⁰ *See Doe I v. Individuals*, 561 F. Supp. 2d 249, 256-57 (D. Conn. 2008) (allowing plaintiffs to pierce defendant's right to speak anonymously where the plaintiff presented a

Moreover, plaintiffs need not prove “actual malice” if the alleged defamation involves the personal affairs of private individuals.³³¹ First Amendment doctrine requires plaintiffs to show “actual malice” only if the plaintiffs are “public figures”³³² or if the statements concern matters on which the public has a justified and important interest.³³³ For instance, in *Time, Inc. v. Firestone*, the Court found no need for proof of “actual malice” in a defamation case concerning the plaintiff’s divorce because the dissolution of a marriage does not involve a matter of public interest, even though the marital difficulties of wealthy individuals might be of some interest to the public, and because the plaintiff did not freely choose to publicize issues related to her married life.³³⁴

Few of the targets of online mobs are likely to be “public figures” even for special purposes: their influence is simply too minimal to suggest they “have assumed roles of especial prominence in the affairs of society.”³³⁵ A person whose published writings reach a relatively small category of people in a particular field is not a public figure.³³⁶ Nor do the public controversies that surround attacks, and victims’ attempts to defend themselves, render them public figures: “[T]hose charged with defamation cannot, by their own conduct, create their own defense by making the claimant a public figure.”³³⁷ Moreover, the assaults often involve highly personal matters on which the public lacks an important interest. If the public does not have an important interest in learning about the divorce of a wealthy couple, it surely has no interest in charges of private individuals’ sexually transmitted diseases or mental illnesses. Thus, victims such as students and bloggers would not have to prove actual malice to pursue defamation claims.

prima facie case of defamation in which the defendant falsely claimed that plaintiff, a female law student, had a gay affair with a law school administrator, because the statement would harm the plaintiff’s reputation).

³³¹ *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 762-63 (1985) (finding no “actual malice” requirement in a defamation case about an erroneous credit report issued for plaintiff company because it did not concern an issue in which the public had a justified and important interest); *Time, Inc. v. Firestone*, 424 U.S. 448, 453-55 (1976).

³³² *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 345 (1974) (refusing to require actual malice in a defamation case involving a private figure who did not thrust himself into the vortex of a public issue).

³³³ *Curtis Publ’g Co. v. Butts*, 388 U.S. 130, 155 (1967) (explaining that the burden of proving “actual malice” is predicated in large part on the assumption that public figures have sufficient access to the media to defend themselves); *N.Y. Times Co. v. Sullivan*, 376 U.S. 254, 266 (1964).

³³⁴ *Time, Inc.*, 424 U.S. at 453-54.

³³⁵ See *Gertz*, 418 U.S. at 345 (refusing to deem a well-known attorney as a public figure).

³³⁶ *Hutchinson v. Proxmire*, 443 U.S. 111, 135 (1979).

³³⁷ *Id.*

Free speech doctrine would also not limit emotional distress claims, as the attacks here mainly involve private individuals, rather than public figures. Only in cases involving “public debate about public figures” does First Amendment doctrine require proof that “the publication contains a false statement of fact which was made with ‘actual malice.’”³³⁸ As with defamation claims, the actual malice standard does not apply to a private person whose emotional distress concerns personal matters.³³⁹ Many of the women targeted online, such as the female law students, would not be considered public figures because they never sought to attract the public’s attention. Although some victims, such as Kathy Sierra, might be considered public figures due to their especial prominence, the assaults do not address issues of public concern and thus may be actionable without showing actual malice.

2. Civil Rights Law

Civil rights violations have a dual character. On one hand, they single out people of color, religious minorities, women, and other traditionally subjugated groups for abuse that wreaks special harm on the victims and their communities. On the other hand, they explicitly or implicitly communicate a racist or otherwise bigoted viewpoint. The Court has made clear that the First Amendment poses no obstacle to punishing a defendant for his decision to target vulnerable individuals for abuse because of their gender or race, and for the grave harm the targeting of vulnerable individuals inflicts. Moreover, the Court has refused to allow perpetrators to immunize actions by adding some explicit expressions. The Court has, however, rejected attempts to proscribe abusive expressions solely because their content may be more offensive to vulnerable people. This viewpoint discrimination restriction poses little

³³⁸ See, e.g., *Hustler Magazine, Inc. v. Falwell*, 485 U.S. 46, 53, 56 (1988) (finding no actionable intentional infliction of emotional distress claim where a magazine advertisement suggested the plaintiff, a nationally known minister, had a “drunken incestuous rendezvous with his mother in an outhouse”). The actual malice standard does apply to private individuals who have thrust themselves into the public sphere. E.g., *Gilbert v. Sykes*, 53 Cal. Rptr. 3d 752, 762-63 (Ct. App. 2007) (requiring proof of actual malice in an emotional distress case involving online criticism of a plastic surgeon, because the surgeon had cast himself into the public sphere “by appearing on local television shows[,] . . . writing numerous articles in medical journals and beauty magazines, . . . [and testifying] as an expert witness”).

³³⁹ See, e.g., *Inland Mediation Bd. v. City of Pomona*, 158 F. Supp. 2d 1120, 1158 n.30 (C.D. Cal. 2001); *State v. Carpenter*, 171 P.3d 41, 56 (Alaska 2007). To be sure, the First Amendment would bar an emotional distress claim based solely on the content of constitutionally protected statements, such as privileged opinion. *Hustler*, 485 U.S. at 55-56. The emotional distress claims envisioned here, however, would not be based upon protected opinion, but rather upon intimidating and frightening threats of physical violence, the posting of Social Security numbers, and alleged lies about verifiable facts, such as a victim’s sexual health.

obstacle to the pursuit of federal and state antidiscrimination actions against online mobs.

The two leading cases in this area are *R.A.V. v. City of St. Paul*³⁴⁰ and *Wisconsin v. Mitchell*.³⁴¹ In *R.A.V.*, the city criminalized conduct that an individual “knows or has reasonable grounds to know arouses anger, alarm or resentment in others on the basis of race, color, creed, religion, or gender.”³⁴² The Court held that this ordinance unconstitutionally discriminated on the basis of the content of certain offensive expressions – expressions that offensively demonstrated bigoted ideas were proscribed by the ordinance, yet those that gave offense in other ways were not.³⁴³ The Court explained:

Displays containing abusive invective, no matter how vicious or severe, are permissible unless they are addressed to one of the specified disfavored topics. Those who wish to use “fighting words” in connection with other ideas – to express hostility, for example, on the basis of political affiliation, union membership, or homosexuality – are not covered. The First Amendment does not permit St. Paul to impose special prohibitions on those speakers who express views on disfavored subjects.³⁴⁴

The government cannot discriminate on the basis of the ideas expressed, even within categories of speech and conduct that the First Amendment does not protect independently.³⁴⁵ Thus, it can prohibit all obscene or defamatory statements, or all fighting words, but not only those conveying a particular type of message independent of their obscene, defamatory, or incendiary character.³⁴⁶

The Court emphasized the narrowness of its findings by explicitly upholding several civil rights laws prohibiting sexual harassment in the workplace, even though that type of harassment is commonly accomplished through expressions that are far more likely to be misogynistic than feminist.³⁴⁷ It explained that Congress directed Title VII’s prohibition on “sexually derogatory ‘fighting words’” at conduct and thus its “content-based subcategory of a proscribable class of speech [is] swept up incidentally within the reach of a statute directed at conduct rather than speech.”³⁴⁸ Also acceptable are laws that focus on those expressions most likely to cause harm, so long as those laws do not define

³⁴⁰ 505 U.S. 377 (1992).

³⁴¹ 508 U.S. 476 (1993).

³⁴² *R.A.V.*, 505 U.S. at 380 (citing ST. PAUL, MINN., BIAS-MOTIVATED CRIME ORDINANCE § 292.02 (1990)).

³⁴³ *Id.* at 391.

³⁴⁴ *Id.*

³⁴⁵ *Id.* at 383-84.

³⁴⁶ *Id.* at 384.

³⁴⁷ *Id.* at 389.

³⁴⁸ *Id.*

harmfulness in terms of the viewpoint expressed.³⁴⁹ More generally, the Court explained that “[w]here the government does not target conduct on the basis of its expressive content, acts are not shielded from regulation merely because they express a discriminatory idea or philosophy.”³⁵⁰

A year later, in *Mitchell v. Wisconsin*, a unanimous Court confirmed that *R.A.V.*'s holding was narrow indeed. *Mitchell* involved a Wisconsin statute allowing harsher sentences for certain crimes if the perpetrator selected his or her victim “because of . . . race, religion, color, disability, sexual orientation, national origin or ancestry.”³⁵¹ A unanimous Court rejected the defendant's claim that the statute discriminated against him on the basis of his racist views.³⁵² It noted that the additional penalties attached to the defendant's discriminatory intent because of his conduct, not his bigoted ideas.³⁵³

The Court analogized the Wisconsin statute to federal and state antidiscrimination laws, which, it explained, were immune from First Amendment challenge.³⁵⁴ It pointed to Title VII of the Civil Rights Act of 1964 and 42 U.S.C. § 1981 as examples from civil rights law of “permissible content-neutral regulation of conduct.”³⁵⁵ The Court noted that “whereas the ordinance struck down in *R.A.V.* was explicitly directed at expression (*i.e.*, ‘speech’ or ‘messages’), the statute in this case is aimed at conduct unprotected by the First Amendment.”³⁵⁶ It found Wisconsin was justified in singling out “bias-inspired conduct because this conduct is thought to inflict greater individual and societal harm. . . . The State's desire to redress these perceived harms provides an adequate explanation for its penalty-enhancement provision over and above mere disagreement with offenders' beliefs or biases.”³⁵⁷ The Court underscored that “[t]he First Amendment . . . does not prohibit the evidentiary use of speech to establish the elements of a crime or to prove motive or intent.”³⁵⁸

Applying civil rights statutes to the attacks of cyber mobs falls clearly on the *Mitchell* side of this line. The statutes' proscriptions turn on an online mob's discriminatory choice of victim and the distinct harm to victims and society that the defendant's abusive conduct produces, rather than on the opinions that either the victims or the attackers express.³⁵⁹ Seeking to prevent a woman from maintaining an income-generating blog through threats and denial-of-

³⁴⁹ *Id.* at 388.

³⁵⁰ *Id.* at 390.

³⁵¹ *Wisconsin v. Mitchell*, 509 U.S. 476, 480 (1993).

³⁵² *Id.* at 487.

³⁵³ *Id.* at 487-88.

³⁵⁴ *Id.* at 487.

³⁵⁵ *Id.*

³⁵⁶ *Id.* (citation omitted).

³⁵⁷ *Id.* at 487-88.

³⁵⁸ *Id.* at 489.

³⁵⁹ See Lawrence, *Resolving Paradox*, *supra* note 280, at 721.

service attacks because she is a woman is equally offensive, and equally proscribed, no matter the perpetrator's specific views. Aiming to prevent a person of color from securing gainful employment because of her race is no more or less offensive depending on the nature of the lies or the private information disseminated. Many online attacks have included racist, sexist, or other bigoted language; others have not. When the law punishes online attackers due to the special severity of the social harm produced by targeting these classes of victims on bases of gender or race, and not due to the particular opinions the victims express, no First Amendment values are implicated.

R.A.V. confirmed "that nonverbal expressive activity can be banned because of the action it entails, but not because of the ideas it expresses."³⁶⁰ The application of civil rights laws to online mobs clearly targets actions – the interference with job opportunities through threats, damaging statements, and technological attacks – and is indifferent to the mobs' ideas. Indeed, even if these laws did single out some sub-types of proscribed speech, such as severe threats or especially injurious defamation, the Court noted that it would raise no First Amendment concerns. The Court explained:

When the basis for the content discrimination consists entirely of the very reason the entire class of speech at issue is proscribable, no significant danger of idea or viewpoint discrimination exists. Such a reason, having been adjudged neutral enough to support exclusion of the entire class of speech from First Amendment protection, is also neutral enough to form the basis of distinction within the class.³⁶¹

*Virginia v. Black*³⁶² provides further support for this reading of *R.A.V.* In *Black*, the Court held that a state "may ban cross burning carried out with the intent to intimidate," but struck down a provision in Virginia's statute that treated all cross-burnings as prima facie evidence of intent to intimidate.³⁶³ The Court explicitly reaffirmed *R.A.V.*'s holding that the government may prohibit low-value speech across-the-board, but not specific speech that

³⁶⁰ *R.A.V. v. City of St. Paul*, 505 U.S. 377, 385 (1992).

³⁶¹ *Id.* at 388. The Court found nothing problematic about banning only the most prurient obscenity and threats to the most senior public officials, or allowing states to regulate price advertising in an industry deemed particularly prone to fraud. *Id.* It explained that a federal statute criminalizing only threats of violence made against the President would be upheld because it serves the reasons why such threats fall "outside the First Amendment ([e.g.,] protecting individuals from the fear of violence, from the disruption that fear engenders, and from the possibility that the threatened violence will occur)" in the first place. *Id.* On the other hand, a federal law that only criminalized threats of violence mentioning the President's policy on aid to inner cities would be unconstitutional as its content discrimination would not fall within the reasons why threats of violence are outside the First Amendment. *Id.*

³⁶² 538 U.S. 343 (2003).

³⁶³ *Id.* at 347-48.

discriminates on the basis of message.³⁶⁴ The Court distinguished cross-burning with the intent to intimidate, which it deemed a proscribable “true threat,” from cross-burning for other purposes, which it held constituted a protected expression of a viewpoint.³⁶⁵ Thus, far from being immune from scrutiny, *Black* confirms that actors’ motives may be decisive in the classification of their actions.³⁶⁶ This is precisely the point that *Mitchell* made.

Attempting to prevent anyone from making a living is offensive. By contrast, attempting to prevent someone from making a living because of her race is a civil rights violation. Federal and state antidiscrimination laws focus on the perpetrator’s discriminatory intent in targeting the victim and the special harm that results, not on any views that either the perpetrator or victim might have, and thus the laws’ application here would not offend the First Amendment. As such, their application to online mobs poses no First Amendment problems under current doctrine.

IV. THE ROLE OF WEBSITE OPERATORS

Throughout history, technological advances have created large, successful business entities. Those harmed by new technologies see these entities as fitting sources of compensation for their injuries. As new technologies come to permeate society, these large businesses inevitably facilitate anti-social, as well as pro-social, behavior. For instance, the building of canals, railroads, and reservoirs at the dawn of the Industrial Revolution contributed much to the economy, yet also inflicted waves of destruction on adjoining property owners and towns, much of it wholly unnecessary.³⁶⁷

The law’s reaction to claims against large actors for new types of harms typically goes through three distinct phases. First, it recognizes the new form of harm, but not the benefit that the new technology has occasioned.³⁶⁸ This drives the law to adapt existing theories of liability to reach that harm. Second, after the technology’s benefits become apparent, the law abruptly reverses course, seeing its earlier awards of liability as threats to technological progress and granting sweeping protection to the firms in the new industry.³⁶⁹ Finally,

³⁶⁴ *Id.* at 361-63.

³⁶⁵ *Id.* at 365.

³⁶⁶ See Lawrence, *Evolving Role*, *supra* note 206, at 269.

³⁶⁷ See HORWITZ, *supra* note 29, at 71-74.

³⁶⁸ See *id.* at 85 (explaining that “at the beginning of the nineteenth century, there was a general private law presumption in favor of compensation”).

³⁶⁹ Citron, *supra* note 43, at 273-76. For instance, courts in the newly industrialized America refused to follow the British decision of *Rylands v. Fletcher*, (1868) 3 L.R.E. & I. App. 330 (H.L.), which adopted a strict-liability approach for damage caused by bursting reservoirs, because of a fear that the cost of faultless accidents would preclude the growth of fledgling industry. *Brown v. Collins*, 53 N.H. 442, 448 (1873) (finding *Rylands* antithetical to “progress and improvement”); FRIEDMAN, *supra* note 3, at 351 (explaining how absolute

once the technology becomes better established, the law recognizes that not all liability awards threaten its survival.³⁷⁰ It then separates activities that are indispensable to the pursuit of the new industry from behavior that causes unnecessary harm to third parties.³⁷¹ This is, for example, what the celebrated *Palsgraf v. Long Island Railroad Co.*³⁷² case accomplished and much of the reason the negligence standard emerged. As the new technology progresses and becomes more familiar, the law refines the distinction between acceptable and unacceptable harms, at times setting liability rules to drive the development of less destructive means of carrying out the necessary functions.

This familiar pattern can be seen with regard to the liability of relatively large online actors for harm inflicted through their facilities. The first, hyper-vigilant, stage can be seen in a few early cases, notably *Stratton-Oakmont, Inc. v. Prodigy Co.*, in which courts found ISPs liable for offensive material that came through their portals.³⁷³ Ironically, Prodigy's liability was based in part on its attempt to screen out troubling material, causing the court to reason by analogy from edited newspapers that incur responsibility as publishers for their content.³⁷⁴ The courts' use of an ISP's good faith remedial measures to establish liability disturbed Congress, prompting its passage of § 230 of the Communications Decency Act of 1996 to immunize such actions.³⁷⁵

This legislation merely checked a particular excess of law's hyper-vigilant stage. The law reached the second, hyper-protective stage later, as some courts read § 230 to grant sweeping immunity far beyond what its words and context supported.³⁷⁶ This reaction reached its ironic apogee when courts read a

liability rules, like that imposed in *Rylands*, were initially rejected in the United States because they risked strangling the economy).

³⁷⁰ See, e.g., Citron, *supra* note 43, at 276-77 (explaining that a strong majority of U.S. courts adopted the strict-liability approach of *Rylands* at the turn of the twentieth century because it no longer seemed enterprise-inhibiting).

³⁷¹ *Id.*

³⁷² 162 N.E. 99, 101 (N.Y. 1928).

³⁷³ *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710, at *4-5 (N.Y. Sup. Ct. May 24, 1995).

³⁷⁴ *Id.* at *4.

³⁷⁵ 47 U.S.C. § 230(c)(1) (2000) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

³⁷⁶ See, e.g., *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 333-34 (4th Cir. 1997). The Communications Decency Act consisted of a broad attack on sexually explicit material disseminated through various media. S. REP. NO. 104-23, at 59 (1995). When Congress addressed private actors, as it did in § 230, it was to "encourage telecommunications and information service providers to deploy new technologies and policies" to block offensive material. *Id.* Representatives Christopher Cox and Ron Wyden, who proposed § 230 in a floor amendment, focused on removing impediments to "Good Samaritan" ISPs supplementing the law's protections against obscene and indecent material. H.R. REP. NO. 104-223, at 3, 14 (1995). The Cox-Wyden amendment immunized "action voluntarily taken

provision offering “[p]rotection for private blocking and screening of offensive material”³⁷⁷ to shield operators of sites purveying precisely such material.³⁷⁸ These efforts to read a sweeping immunity into § 230 despite its language and purpose have prevented the courts from exploring what standard of care ought to apply to ISPs and website operators.

This Part seeks to help move the law to the third, more analytical stage. It opposes holding ISPs liable merely because of their deep pockets and inevitable proximity to harm. It is sympathetic to the results, if not the reasoning, of many cases rejecting liability.³⁷⁹ On the other hand, it equally opposes blanket grants of immunity that leave innocent victims of cyber civil rights violations without effective recourse. Instead, this Part seeks to establish a reasonable standard of care that will reduce opportunities for abuses without interfering with the further development of a vibrant Internet or unintentionally converting innocent ISPs or website operators into involuntary insurers of those injured through their sites. Approaching the problem in this manner – as a question of setting an appropriate duty of care – more readily allows for differentiating between disparate kinds of online actors by setting different rules for websites established to facilitate mob attacks, and those large ISPs that beneficially link millions to the Internet. Reaching this stage, however, requires abandoning the hyper-protective stage in which many courts are currently mired.

in good faith to restrict access to material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.” *Id.* at 14. This immunity would combat the problem created by holding ISPs liable for inexact screening – namely, that it discourages intermediaries from engaging in screening in order to distance themselves from the content on their sites, and hence any liability. Susan Freiwald, *Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation*, 14 HARV. J.L. & TECH. 569, 595-96 (2001). The absence of self-screening was antithetical to supporters of the Communications Decency Act, who believed that controlling the volume of noxious material on the Internet exceeded the capacity of public regulatory agencies. 141 CONG. REC. H8469-70 (daily ed. Aug. 4, 1995) (remarks of Rep. Cox). Supporters believed that reducing objectionable material on the Internet depended upon ISPs acting as Good Samaritans, voluntarily screening out as much offensive content as possible. *Id.* Given this history, courts could have limited § 230’s application to intermediaries and websites that engaged in good faith, though incomplete, monitoring. Instead, they interpreted § 230 as absolving intermediaries and website operators of all responsibility for users’ actions, even those that knew about and ignored indecent material. *E.g.*, *Chi. Lawyers’ Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666, 669, 671-72 (7th Cir. 2008).

³⁷⁷ 47 U.S.C. § 230.

³⁷⁸ *See, e.g., Chi. Lawyers’ Comm.*, 519 F.3d at 669, 671-72 (7th Cir. 2008) (finding that a website, designated a non-publisher by § 230(c)(1), could not be held liable under 42 U.S.C. § 3604(c) (2006) for the posting of discriminatory housing advertisements).

³⁷⁹ *See, e.g., Ben Ezra, Weinstein, & Co. v. Am. Online Inc.*, 206 F.3d 980, 983 (10th Cir. 2000) (rejecting a suit against an ISP for alleged negligence in making available stock information concededly provided by known third parties).

Section A demonstrates that granting website operators blanket immunity would be anomalous and undesirable, effectively shielding most online mobs from responsibility for the harm they do. Section B then considers how we ought to construe the standard of care for ISPs and website operators.

A. *Should Website Operators Have Immunity?*

Participants in online mobs may be civilly and criminally liable on a number of bases.³⁸⁰ In practice, however, victims of online mobs may be unable to press their claims against posters who cannot be identified. This can occur if the posters used anonymizing technologies or if the websites hosting the attacks failed to track IP addresses. To be sure, as Jonathan Zittrain points out, “[i]t’s a cat and mouse game of forensics, and if people don’t go to some effort to stay anonymous, it’s frequently possible to figure out who they are.”³⁸¹ All too often, however, abusive posters cover their tracks.

Consider the AutoAdmit case, where the plaintiffs have been unable to identify most of their attackers because AutoAdmit does not log visitors’ IP addresses.³⁸² Although the court has ordered expedited discovery to allow the plaintiffs to locate the anonymous posters, finding them may be impossible due to the fact that ISPs routinely delete data every sixty days.³⁸³ Plaintiffs have posted several messages on AutoAdmit “requesting that defendants come forward for the purpose of being served with the complaint.”³⁸⁴ Not surprisingly, most have not responded.³⁸⁵

Efforts to rein in online mobs may falter if the posters cannot be held responsible for their torts and crimes.³⁸⁶ Generally, the operators of destructive websites either have information that could identify abusive posters or have made a conscious decision not to obtain or retain that information.³⁸⁷ Some

³⁸⁰ See *supra* Part II.A.2.

³⁸¹ Posting of Amir Efrati to Wall Street Journal Law Blog, <http://blogs.wsj.com/law/2008/01/30/subpoena-allowed-in-autoadmit-suit/> (Jan. 30, 2008, 9:08).

³⁸² Posting of Nate Anderson to Ars Technica <http://arstechnica.com/news.ars/post/20080127-yale-students-unable-to-identify-anonymous-forum-bashers.html> (Jan. 27, 2008, 22:39).

³⁸³ Plaintiffs’ Memorandum of Law In Support of Motion for Expedited Discovery at 12 n.80, *Doe I v. Ciolli*, No. 3:07CV00909(CFD) (D. Conn. Jan. 24, 2008), available at http://s.wsj.net/public/resources/documents/WSJ_DEF_MemoofLawreM_012408.pdf [hereinafter *Memo for Expedited Discovery*].

³⁸⁴ *Id.* at 11.

³⁸⁵ Anderson, *supra* note 382. At least one defendant has come forward and filed a motion to quash a subpoena duces tecum issued to AutoAdmit’s ISP for information relating to his identity and a motion to proceed anonymously in the litigation. *Doe I v. Individuals*, 561 F. Supp. 2d 249, 250, 257 (D. Conn. 2008). Both motions were denied. *Id.*

³⁸⁶ See, e.g., *Doe v. GTE Corp.*, 347 F.3d 655, 656 (7th Cir. 2003) (describing the dismissal of anonymous online abusers for the inability to serve).

³⁸⁷ JuicyCampus.com and AutoAdmit.com are prominent examples of such an approach.

website operators function as crowd leaders, influencing the mobs' destructiveness.³⁸⁸ Deterring websites devoted to abusive attacks on individuals plays a crucial role in inhibiting a destructive mob's coordination and efficacy. Thus, holding accountable the operators of websites which facilitate anonymous attacks may hold the key to protecting the civil rights of the women, people of color, and others set upon by online mobs.

By contrast, broad immunity for operators of abusive websites would eliminate incentives for better behavior by those in the best position to minimize harm.³⁸⁹ As Daniel Solove notes, such immunity "can foster irresponsibility."³⁹⁰ With blanket immunity, site operators would have no reason to take down false or injurious material³⁹¹ or to collect and retain the identities of posters.³⁹² As a result, objectionable posts remain online and searchable by employers, often migrating across the web to become effectively irretrievable, while plaintiffs continue to be unable to find and recover damages from wrongdoers.

Supporters of blanket immunity for website operators have several responses to this argument. First, some contend that holding website operators liable is unnecessary, as victims can identify and sue members of online mobs.³⁹³ On some occasions, particularly if victims sue very quickly and persuade the court to order expedited discovery, they may be able to obtain records identifying mob members before ISPs routinely purge their records after sixty days.³⁹⁴ To be sure, the plaintiffs in the AutoAdmit case have

³⁸⁸ See *supra* Part I.B.

³⁸⁹ See Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 224 (2006); Mark A. Lemley, *Rationalizing Internet Safe Harbors* 14 (Stanford Pub. Law, Working Paper No. 979836, 2007), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=979836.

³⁹⁰ SOLOVE, *supra* note 4, at 159.

³⁹¹ Lemley, *supra* note 389, at 16.

³⁹² See *id.*; *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 328 (4th Cir. 1997). *Zeran*, for example, involved an anonymous poster who offered t-shirts that made fun of the Oklahoma City terrorist bombing less than a week after it occurred, and said the t-shirts were available at the plaintiff's phone number. *Id.* at 329. As a result, *Zeran* received a constant stream of abusive calls and death threats. *Id.* Although AOL eventually removed the postings, it never identified the perpetrator. *Id.*

³⁹³ This argument against liability is the equivalent of the now-discredited Fellow Servant Rule which, during the Industrial Revolution, absolved employers of liability for workers' injuries most proximately caused by another worker. FRIEDMAN, *supra* note 3, at 223. Because other workers were almost always more directly involved with injured workers than factory managers, this rule effectively precluded meaningful recoveries for injuries and left unsafe working conditions undeterred. *Id.* at 224. Here, ignoring the website operators' roles because the anonymous posters' behavior is more spectacular is likely to prevent recovery in most cases and leave online mobs largely undeterred.

³⁹⁴ See Memo for Expedited Discovery, *supra* note 383, at 12 n.80.

identified a few of the posters who attacked them.³⁹⁵ Nevertheless, the great majority of defendants seem unlikely to be identified.

Absolving website operators of responsibility when they create sites to facilitate anonymous online attacks will largely foil recovery and eliminate deterrence. Most victims are likely never to have their day in court if website operators are free to facilitate anonymous posting, as victims are typically ordinary individuals unsophisticated in the legal system, the attorneys they consult may be unaware of the data destruction practices that make filing rapidly and seeking expedited discovery so urgent, and judges may not grasp the need to act with such speed at the outset of litigation. Without liability of website operators, victims of online mobs face a de facto statute of limitations of less than sixty days, far less than that applied to other plaintiffs with similar claims.³⁹⁶

Second, some fear over-deterrence: the concern that website operators would automatically remove posts that may stir complaints and hence chill speech, even if the complaints are frivolous.³⁹⁷ This concern is real and merits consideration in crafting the substantive expectations for website operators. Speculation about possible over-deterrence of speech, however, is not a legitimate basis for immunizing a broad class of destructive behavior that itself chills important speech. Any time the law acts to deter destructive behavior, over-deterrence is possible. Even a well-balanced policy may over-deter on some occasions and under-deter on others. The acceptability of those respective errors depends on the values we attach to the problematic conduct and to the potential harm. Eliminating all deterrence based on an unsubstantiated fear that some beneficial conduct might be over-deterred completely devalues the injuries of the women, people of color, and other vulnerable individuals targeted by online mobs. Any over-deterrence – or continued under-deterrence – can be assessed and offset by adjusting the standard of liability, as the Supreme Court did in *New York Times Co. v. Sullivan*.³⁹⁸ Other nations, such as Great Britain and Ireland, do not immunize operators for website content produced by third parties and yet still generate vibrant online discourse.³⁹⁹

A third possible argument for immunizing website operators is to discourage litigation. To be sure, other areas of Internet law seek alternatives to

³⁹⁵ Plaintiffs recently located an ISP with identifying information on one poster and have previously identified five others. The district court upheld a subpoena duces tecum for those records. *Doe I v. Individuals*, 561 F. Supp. 2d 249, 257 (D. Conn 2008).

³⁹⁶ This rule also could promote unnecessary litigation by compelling victims to sue at the first sign of trouble without allowing significant time for investigation or negotiation.

³⁹⁷ SOLOVE, *supra* note 4, at 1243; *Zeran*, 129 F.3d at 333.

³⁹⁸ 376 U.S. 254, 279-83 (1964) (imposing a heightened standard for defamation involving public figures as opposed to private individuals).

³⁹⁹ See Michael L. Rustad & Thomas H. Koenig, *Harmonizing Cybertort Law for Europe and America*, 5 J. HIGH TECH. L. 13, 47-49 (2005).

litigation.⁴⁰⁰ These alternative dispute resolution mechanisms, however, address problems in which ex post remedies are relatively effective and where deterrence is not vital. Online mobs, however, do not operate in good faith. If undeterred, they will continue their attacks, quite willing to have some postings removed – often only after their victims suffer irreparable reputational injuries and the malicious postings have spread across the Internet. Avoidance of unnecessary litigation is a legitimate and important goal, but it too is best addressed in setting the standard of conduct expected from website operators.

Finally, some believe immunizing website operators is essential to preserve anonymity, which they view as vital to free expression on the Internet.⁴⁰¹ They may invoke the role of websites such as Wikileaks.org to facilitate political dissidence against oppressive regimes or analogize to important roles played offline by “anonymous” persons, such as investigative journalists’ sources.⁴⁰² These parallels, however, are inapt. In some instances, many “anonymous” actors are not, in fact, anonymous, but rather have undisclosed identities. No responsible newspaper publishes material based on sources whose identity it does not know. Similarly, although the Supreme Court has rejected thinly supported demands for the production of dissident groups’ membership lists,⁴⁰³ it has never suggested that authorities or private litigants could not obtain the identities of persons reasonably suspected of unlawful activities.⁴⁰⁴ Freedom of expression has never depended on the absolute ability of speakers to prevent themselves from being identified and held responsible for activities the state

⁴⁰⁰ Frank Pasquale, *Asterisk Revisited: Debating a Right of Reply on Search Results*, 3 J. BUS. & TECH. L. 61, 64 (2008) (arguing that informal mechanisms can be an effective first step towards resolving online disputes). Pasquale offers informal processes as a first-step towards accountability in cases involving disputed search engine results. *Id.* For instance, the Uniform Dispute Resolution Policy resolves domain names disputes. *Id.* See generally Jeffrey M. Samuels & Linda B. Samuels, *Internet Domain Names: The Uniform Dispute Resolution Policy*, 40 AM. BUS. L.J. 885 (2003). Additionally, eBay’s internal administrative processes manage disputes among individuals without expensive litigation. Pasquale, *supra*, at 65; see also Mark A. Lemley & R. Anthony Reese, *A Quick and Inexpensive System for Resolving Peer-to-Peer Copyright Disputes*, 23 CARDOZO ARTS & ENT. L.J. 1, 3-4 (2005) (proposing an amendment to the copyright statute that gives a copyright owner “the option to enforce her copyrights *either* by pursuing a civil copyright infringement claim in federal court *or* by pursuing a claim in an administrative dispute resolution proceeding before an administrative law judge in the Copyright Office”).

⁴⁰¹ See SOLOVE, *supra* note 4, at 140.

⁴⁰² Similarly, Congress is considering the proposed Global Online Free Expression Act to ensure the anonymity of political dissidents from oppressive regimes. CTR. FOR DEMOCRACY & TECH., ANALYSIS OF THE GLOBAL ONLINE FREE EXPRESSION ACT OF 2008, at 1 (2008), <http://www.cdt.org/international/censorship/20080505gofa.pdf>.

⁴⁰³ *Bates v. City of Little Rock*, 361 U.S. 516, 527 (1960); *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 466 (1958).

⁴⁰⁴ Indeed, it has gone much further, allowing the state to obtain the Ku Klux Klan’s membership list to deter violence. *New York ex rel. Bryant v. Zimmerman*, 278 U.S. 63, 72 (1928).

may properly prohibit. As Professor Tribe notes, “secrecy often seems the shield of dangerous and irresponsible designs.”⁴⁰⁵

B. *On What Bases Should Website Operators Be Liable?*

The Ninth Circuit has recently noted:

The Internet is no longer a fragile new means of communication that could easily be smothered in the cradle by overzealous enforcement of laws and regulations applicable to brick-and-mortar businesses. Rather, it has become a dominant – perhaps the preeminent – means through which commerce is conducted. And its vast reach into the lives of millions is exactly why we must be careful not to exceed the scope of the immunity provided by Congress and thus give online businesses an unfair advantage over their real-world counterparts, which must comply with laws of general applicability.⁴⁰⁶

On the other hand, rejecting website operators’ extravagant claims of immunity should not lead to a regression to the hyper-vigilant response to web technology represented by *Prodigy*. Instead, it should open the door to the reasoned development of an appropriate standard of care.⁴⁰⁷ The Seventh Circuit, skeptical about assertions of blanket immunity under § 230(c)(1) and echoing many of the concerns raised above, undertook such an inquiry.⁴⁰⁸ It failed, however, to appreciate the important differences between ISPs and other communications media in allowing wrongdoers to conceal their identity and escape liability for their actions.⁴⁰⁹

Treating website operators as distributors of defamatory material could require them to remove offensive posts when notified by victims.⁴¹⁰ In practice, however, notice-and-takedown regimes have not worked well in other

⁴⁰⁵ TRIBE, *supra* note 285, at 1019.

⁴⁰⁶ *Fair Housing Council v. Roommates.com, L.L.C.*, 521 F.3d 1157, 1164-65 n.15 (9th Cir. 2008).

⁴⁰⁷ In particular, because some cases have involved non-anonymous or only thinly veiled posters, and because courts have so focused on liability for developing offensive material to address overbroad readings of 47 U.S.C. § 230(c)(1), they have given scant consideration to liability for helping online malefactors escape liability. *See, e.g., id.* at 1174-75.

⁴⁰⁸ *Doe v. GTE Corp.*, 347 F.3d 655, 659-62 (7th Cir. 2003).

⁴⁰⁹ *See id.*

⁴¹⁰ *Cf.* Posting of Orin Kerr to The Volokh Conspiracy, <http://volokh.com/posts/1176705254.shtml> (Apr. 16, 2007, 17:11) (suggesting that website operators could de-index malicious postings so that they would not be searchable). Website operators can use common Web protocols to request that search engines do not index particular pages. Under this approach, site operators would either take full responsibility for content on their sites or keep it out of search engines to mitigate the harm to a victim’s privacy and reputation. *Id.*

contexts, such as the Digital Millennium Copyright Act.⁴¹¹ The difficulty of such a regime is two-fold. First, it has the potential to sweep too broadly. Once notified of a complaint, ISPs and website operators might take down postings simply to avoid liability, no matter how innocuous the postings might be. Second, such a regime would be ineffective, because by the time a victim realizes the problem, notifies the website operator, and has the material removed, it may have spread to other sites, becoming effectively impossible to contain.⁴¹² At best, these regimes would modestly mitigate the still-substantial harm done by online mobs. Malicious posters would have no reason to refrain from acting abusively in the future, and the website operators would have no reason to change the configuration of their websites to hamper further anonymous attacks. Conversely, common targets of online mobs would continue to have reason to fear blogging in their own names or even speaking out offline in settings where they could irritate persons that might retaliate online. Something different is needed to deter online mobs' unlawful conduct.

An orderly articulation of the standard of care for ISPs and website operators is essential. First, it should require website operators to configure their sites to collect and retain visitors' IP addresses.⁴¹³ In other words, the standard of care should demand "traceable anonymity."⁴¹⁴ This would allow posters to comment anonymously to the outside world but permit their identity to be traced in the event they engage in unlawful behavior. Requiring traceable anonymity is hardly a burdensome step: some blogs already deny access to anonymous posters.⁴¹⁵

Traceable anonymity would not betray our commitment to anonymous speech if site operators and ISPs refuse to reveal a poster's identity unless a court order demanded it. This would protect individuals for whom anonymity

⁴¹¹ See, e.g., Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effects?" Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621, 623 (2006) (discussing the high incidence of abuse of the "notice and takedown" process for copyright infringement under 17 U.S.C. § 512(b) (2000)).

⁴¹² See Posting of Ross Tucker to Tech Policy Seminar, http://picker.typepad.com/picker_seminar/2008/04/isp-liability-a.html (Apr. 28, 2008, 12:34).

⁴¹³ Lemley, *supra* note 389, at 22 n.74. It may be reasonable to insist that websites and ISPs retain such data for three years, which should provide plaintiffs sufficient time to investigate and pursue claims. This would accord with many statutes of limitations for tort claims and would not impose a high price tag given the falling costs associated with data storage.

⁴¹⁴ SOLOVE, *supra* note 4, at 146; Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. MIAMI L. REV. 991, 1028-32 (2004).

⁴¹⁵ For instance, the legal blog Concurring Opinions, where I am a permanent member, tracks commentators' IP addresses. See SOLOVE, *supra* note 4, at 146 (describing the traceable anonymity at Concurring Opinions, which he founded).

is most crucial, such as victims of domestic violence and political dissidents. At present, courts protect the identity of anonymous posters from frivolous lawsuits by setting forth a series of requirements before granting *John Doe* subpoenas.⁴¹⁶ Those requirements should, at the very least, include proof that the claims would survive a motion for summary judgment.⁴¹⁷ This would assure posters of the safety of their anonymity in the face of baseless allegations.

A standard of care that includes traceable anonymity would allow society to enjoy the free expression that anonymity facilitates without eliminating means to combat anonymity's dark side – the tendency to act destructively when we believe we cannot get caught.⁴¹⁸ As Justice Scalia has explained, because anonymity makes lying easier, the identification of speakers can significantly deter the spreading of false rumors and allow us to locate and punish the source of such rumors.⁴¹⁹

Second, as screening software advances, some classes of online actors may reasonably be expected to deploy the software to limit the amount and kinds of harmful materials on their sites.⁴²⁰ This certainly is wholly consistent with the Communications Decency Act's objectives. As Susan Freiwald explains, reducing defamation through technological means may be possible if companies invested in code to make it feasible.⁴²¹ Naturally, online actors

⁴¹⁶ *Doe v. Cahill*, 884 A.2d 451, 457 (Del. 2005) (holding that “a defamation plaintiff must satisfy a ‘summary judgment’ standard before obtaining the identity of an anonymous defendant”); Nathaniel Gleicher, Note, *John Doe Subpoenas: Toward a Consistent Standard*, 118 YALE L.J. (forthcoming 2009) (manuscript at 29, on file with the author). Mark Lemley offers an alternative to a *Doe* lawsuit – granting subpoenas upon a showing of good cause without a lawsuit where the ISP or website operator would be required to notify the defendant and give him a chance to contest the subpoena anonymously, either in court or in the administrative process suggested above. Lemley, *supra* note 389, at 21-22. Some extreme libertarians might object on privacy grounds to a standard of care requiring retention of visitors' IP addresses. They might argue that it could facilitate spying and overreaching. As discussed above, the commitment to allowing anonymous speech has never extended to shield criminal or tortious behavior. *See supra* Section IV.A. Moreover, First Amendment considerations are greatly attenuated when it is not the government, but a large number of independent private entities retaining the sensitive information, and where those whose information is held voluntarily chose to visit and post on those websites.

⁴¹⁷ *E.g.*, *Cahill*, 884 A.2d at 457.

⁴¹⁸ SOLOVE, *supra* note 4, at 140; *see also supra* notes 159-160 (discussing deindividuation caused by anonymity).

⁴¹⁹ *McIntyre v. Ohio Election Comm'n*, 514 U.S. 334, 382 (1995) (Scalia, J., dissenting).

⁴²⁰ Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. (forthcoming 2009) (manuscript at 21-22), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1261344 (describing the falling costs and technological advances which have produced deep-packet inspection technologies, allowing ISPs to record and monitor all their consumers' Internet communications, including e-mails, web surfing, instant messages, and the like).

⁴²¹ Freiwald, *supra* note 376, at 629.

would not be liable for the inevitable failures of this software to screen out all offensive material as § 230 demands. But making a reasonable good faith attempt to conduct cost-effective screening could significantly reduce harm.⁴²²

Third, and more generally, the duty of care should take into account differences among online entities. ISPs and massive blogs with hundreds or thousands of postings a day cannot plausibly monitor the content of all postings.⁴²³ The duty of care will also surely evolve as technology improves. Current screening technology is far more effective against some kinds of abusive material than others; progress may produce cost-effective means of defeating other attacks. Conversely, technological advances will likely offer online mobs new means of carrying out their assaults, creating new risks against which victims can ask website operators to take reasonable precautions.

CONCLUSION

Scholars and activists began developing a cyber civil liberties agenda from the earliest days of the Internet. Although preservation of those liberties requires constant vigilance, they have accomplished much. Unfortunately, the Internet's impact on civil rights has gone largely neglected to date. As a result, something with the potential to be a great engine of equality has all too often reflected and reinforced the offline world's power imbalances. The brutality of online mobs is an important part of that story, but it is only a part. Scholars and activists need to devote the same attention to online threats to civil rights that they have to civil liberties. This Article aims to open that discussion.

⁴²² Some kinds of attacks, such as doctored, sexually suggestive pictures, may be easier to screen out than others, such as defamation. Nonetheless, crafting screening algorithms is a sophisticated enterprise; lay judges should be wary of speculating about what can and cannot be accomplished. *See* Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 668 (7th Cir. 2008) (suggesting that racially discriminatory real estate ads cannot be eliminated because offering a "red brick house with white trim" is lawful).

⁴²³ Jack Balkin argues that the risk of unconstitutional collateral censorship is high for entities that do not sit in the best position to detect unlawful activities, including ISPs who cannot oversee the postings of customers, and bookstore owners who cannot possibly inspect all of the books on the shelves. J.M. Balkin, Essay, *Free Speech and Hostile Environments*, 99 COLUM. L. REV. 2295, 2302-04 (1999).