2015

Addressing Cyber Harassment: An Overview of Hate Crimes in Cyberspace

Danielle K. Citron
Boston University School of Law

Addressing Cyber Harassment: An Overview of Hate Crimes in Cyberspace

Danielle Keats Citron

University of Maryland Francis King Carey School of Law
Legal Studies Research Paper
No. 2017-9

ADDRESSING CYBER HARASSMENT: AN OVERVIEW OF HATE CRIMES IN CYBERSPACE

Danielle Keats Citron[*]

INTRODUCTION

It is an auspicious time to discuss cyber harassment and cyber stalking. When I began writing about cyber harassment in 2007, it was dismissed as a part of the bargain of online life. Although the abuse often involved threats, defamation, and privacy invasions, commentators regarded it as "no big deal."[1] Victims were told to stop "whining" because they chose to blog about controversial topics or to share nude images of themselves with confidantes. Victims were advised to toughen up or go offline.[2] The choice was theirs—that was the deal.

Since 2007, so much has changed. Cyber harassment's harms are now part of the national conversation. Perceptions and attitudes have changed,[3] thanks in no small part to the work of *Cyber Civil Rights Initiative*[4] (CCRI), *End Revenge Porn,*[5] and *Without My Consent*,[6] advocacy groups devoted to educating the public about online harassment and to spearheading reform.

---

* Lois K. Macht Research Professor & Professor of Law, University of Maryland Francis King Carey School of Law, Senior Fellow, Future of Privacy, Affiliate Scholar, Stanford Center on Internet & Society, Affiliate Fellow, Yale Information Society Project. I am grateful to Co-Dean Michael Scharf, Professor Ray Ku, Stephen Congdon, and the staff of Case Western University's Journal of Law, Technology, and the Internet who kindly hosted me to talk about my book Hate Crimes in Cyberspace as its first inaugural distinguished speaker. This short piece is adapted from my talk.

1. DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014) at 19. (exploring entrenched social attitudes trivializing cyber harassment); Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373 (2009).

2. DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014) at 19 [hereinafter CITRON].

3. *See generally* Danielle Citron, *Online Engagement on Equal Terms*, B.U. L. REV. (Blog) (Oct. 19, 2015), http://www.bu.edu/bulawreview/citron-online-engagement-on-equal-terms/.

4. *See generally About Us*, CYBER CIVIL RIGHTS INITIATIVE, http://www.cybercivilrights.org/about (last visited Mar. 7, 2016).

5. *See generally Our Mission*, END REVENGE PORN, http://www.endrevengeporn.org/about/ (last visited Mar. 7, 2016).

6. *See generally Who We Are*, WITHOUT MY CONSENT, http://www.withoutmyconsent.org/who-we-are (last visited Mar. 7, 2016).

This short piece will take a step back and give an overhead view of the problem of cyber harassment and the destructive impact it can have on victims' lives. Then, it will address about what the law can do to combat online harassment and how a legal agenda can be reconciled with the First Amendment. Finally, it will turn to recent changes in social media companies' treatment of online abuse and what that might mean for our system of free expression.

I. UNDERSTANDING CYBER HARASSMENT

Cyber harassment involves a persistent and repeated course of conduct targeted at a specific person, that is designed to and that causes the person severe emotional distress, and often the fear of physical harm.[7] Cyber harassment is often accomplished by a perfect storm of abuse.[8] Harassers terrorize victims by threatening violence. They post defamatory falsehoods about victims.[9] They impersonate victims in online ads, and suggest—falsely—that their victims are interested in sex.[10] Sometimes, harassers manipulate search engines to ensure the prominence of the lies in searches of victims' names.[11] Harassers invade victims' privacy by posting their sensitive information, such as nude images or Social Security numbers.[12] Lastly, harassers use technology to knock people offline. [13]

A. Two Women's Stories of Harassment Represent the Broader Phenomenon

In 2012, Anita Sarkeesian, a well-known video game critic, announced that she was raising money on Kickstarter to fund a documentary series about sexism in video games.[14] A week after Sarkeesian made her announcement, a cyber mob descended upon her. On Sarkeesian's blog and Twitter feed, and in her email inbox, she received graphic rape and death threats. Additionally, a game appeared online titled, "Beat Up Anita

7. CITRON, *supra* note 2, at 3. I use the terms cyber harassment and cyber stalking interchangeably in my book, as I do here.

8. *Id*.

9. *Id*.

10. *Id*.

11. *Id*.

12. *Id*.

13. *Id*. at 4.

14. *See* Helen Lewis, *Dear the Internet, This is Why You Can't Have Anything Nice*, NEW STATESMAN (blog) (June 12, 2012, 11:34 AM), http://www.newstatesman.com/blogs/internet/2012/06/dear-internet-why-you-cant-have-anything-nice.

Sarkeesian."[15] Each time a player touched the keyboard, a depiction of Sarkeesian's face grew more bloodied and swollen.[16]

Next, the mob went after Sarkeesian's fundraising effort. Kickstarter received hundreds of false reports that Sarkeesian was engaged in fraud.[17] Harassers tried to get Twitter and Facebook to shut down her accounts by erroneously reporting her profiles as hate speech, spam, and terrorism.[18]

The abuse escalated during the summer of 2014.[19] At the time, women in gaming including Zoe Quinn and Brianna Wu, faced online attacks by a cyber mob claiming that women were ruining games with their political correctness and their influence on journalists covering the industry.[20] During the height of the GamerGate attacks, Ms. Sarkeesian was supposed to give a talk at Utah State University. She canceled her appearance after the University's Dean received threats.[21] The message was that if Ms. Sarkeesian spoke, there would be a school shooting worse than Columbine and Newtown combined.[22]

Not every cyber harassment victim has a public profile like Sarkeesian. Most victims come from everyday walks of life—the teacher, nurse, dentist, and stay-at-home parent. Holly Jacobs was getting her doctorate in industrial psychology when she was targeted with online abuse. Ms. Jacobs shared nude images of herself with a boyfriend during their long-distance relationship. The sharing went both ways; the understanding was that the photos were for their eyes only. After the relationship ended, Ms. Jacobs began receiving emails and texts from strangers saying they saw her online advertisement and wanted to have sex with her.[23] So she did what anyone would do: she Googled herself and what she found was terrifying. On over

15. *See* Kevin Morris, *Anita Sarkeesian Haters Flood TED Talk with Misogynist Comments*, THE DAILY DOT (December 6, 2012), http://www.dailydot.com/culture/anita-sarkeesian-ted-talk-misogynist-comments/.

16. *Id*.

17. Interview with Anita Sarkeesian, September 14, 2013 (notes on file with author).

18. *Id*.

19. E-mail from Anita Sarkeesian to author, January 26, 2014 (on file with author); e-mail from Anita Sarkeesain to author, February 6, 2014 (on file with author).

20. *See* Keith Stewart, *Brianna Wu and the Human Cost of Gamergate*, THE GUARDIAN (Oct. 17, 2014), http://www.theguardian.com/technology/2014/oct/17/brianna-wu-gamergate-human-cost.

21. *See UPDATE: Sarkeesian Event Cancelled*, UTAH STATE UNIVERSITY (Oct. 14, 2014), http://www.usu.edu/today/index.cfm?id=54178.

22. *See* Saeed Ahmed, *Anita Sarkeesian Forced to Cancel Utah State Speech After Mass Shooting* Threat, CNN (Oct. 15, 2014, 10:57 AM), http://www.cnn.com/2014/10/15/tech/utah-anita-sarkeesian-threat/.

23. *See* Holly Jacobs, *A Message from our Founder, Dr. Holly Jacobs*, END REVENGE PORN (Sept. 8, 2013), http://www.endrevengeporn.org/a-message-from-our-founder-holly-jacobs/.

300 sites—revenge porn sites, porn sites, and adult encounter sites—there were her nude photos.[24] Some of the posts said that Ms. Jacobs wanted sex and provided her contact information.[25] Other posts accused Ms. Jacobs of sleeping with undergraduate students at her university. Her part time employer received an email with the nude photos; her Dean of Students received anonymous calls accusing her of sleeping with her students.[26] She tried to get the photos taken down—she took many of the photos and filed DMCA requests. But most of her requests were ignored and the photos stayed online.[27]

B. Female Victims, Gendered Abuse

Anita Sarkeesian and Holly Jacobs's experiences are not unique. According to a study released in 2009, approximately 850,000 people experience cyber harassment a year.[28] The majority of victims are female, but men are targeted too and the playbook of the abuse is often the same.[29] The abuse is sexually threatening and sexually humiliating. Victims face rape threats or threats of anal rape; they are accused of having sexually transmitted diseases and of being available for sex; privacy invasions often involve the posting of nude photos.[30]

The fallout for victims is profound. The professional costs are steep. It can be difficult for victims to keep or get a job because online searches of their names prominently feature the abuse. A 2009 Microsoft study found that over 80% of employers use search engines to research candidates and over 70% of the time there is a negative result.[31] It is not hard to understand why employers would not hire someone struggling with online abuse. It is far easier, safer, and smarter in terms of client perceptions to hire someone who does not come with baggage.

Victims fundamentally change their lives.[32] They move because they no longer feel safe at home, and they often change their names, as Ms.

---

24. *Id*.

25. *Id*.

26. *Id*.

27. *Id*.

28. U.S. DEP'T. OF JUSTICE, BUREAU OF JUSTICE STATISTICS, STALKING VICTIMIZATION IN THE UNITED STATES, SPECIAL REPORT NO. NCJ 224527 (2009), at 8.

29. *Id*.

30. *See generally* CITRON, *supra* note 2.

31. *See* CROSS-TAB, ONLINE REPUTATION IN A CONNECTED WORLD 9 (2010), (available at: http://go.microsoft.com/?linkid=9709510).

32. *See generally* Matt Nobles, Bradford Reyns, Bonnie Fisher, and Kathleen Fox, *Protection against Pursuit: A Conceptual and Empirical Comparison of Cyberstalking and Stalking Victimization among a National Sample*, JUSTICE QUARTERLY (2013) (available at

Jacobs was forced to do. Victims experience severe emotional distress, anxiety, and depression.[33]

Crucially, online attacks can prevent people from engaging and speaking online. Victims shut down their blogs, social network profiles, and websites. They retreat because staying online often makes matters worse. [34]

II. LAW'S POTENTIAL ROLE

Victims may be able to sue their harassers for tort claims: defamation, public disclosure of private fact, and intentional infliction of emotional distress. However, financing these claims is difficult. It is incredibly expensive to bring a private lawsuit, and most victims do not have the resources to hire an attorney. Further, it is even more difficult to convince an attorney to take a case on a contingency basis. There are no deep pockets to go after in cases involving cyber harassment. Under the Federal Communications Decency Act, online platforms are mostly immune from liability for user-generated content.[35]

What about criminal law? At the federal level, there are cyber stalking, cyber harassment, and threat laws. But for too long those laws were under enforced. This is in large part because federal authorities lack the resources to address most online harassment cases. Also, cyber harassment is not a priority. As federal agents told Holly Jacobs, nothing could be done because the attacks were not a matter of national security.[36]

At the state level, at least half of the states have well designed cyber stalking and harassment and threat laws.[37] The problem, however, is law enforcement's lack of familiarity with the technology and the law. Victims are often told to ignore the abuse. For the rest of the states, harassment and stalking laws only cover abuse sent directly to victims—they do not cover nude photos, threats, and lies posted on third party sites, so there is still much work to be done with lawmakers.

What about civil rights law? Cyber harassment should be understood as a civil rights violation if it interferes with people's crucial life opportunities—the ability to work and speak—because of their membership in a protected group. As journalist Amanda Hess poignantly

---

https://repository.asu.edu/attachments/144987/content/Protection%20Against%20Pursuit.pdf).

33. *See* B.J. Lee, *Suicide Spurs Bid to Regulate the Net in South Korea*, NEWSWEEK.COM (October 15, 2008) (available at: http://able2know.org/topic/124046-1).

34. CITRON, *supra* note 2, at 10-11.

35. *Id*. at 25.

36. *Id*. at 86.

37. *Id*. at 83-84.

said, rape threats say to all women they are not welcome online.[38] Still, federal and state civil rights laws need updating. For instance, federal civil rights laws criminalize threats that interfere with someone's employment because of the person's race, religion, or national origin.[39] Gender and sexual orientation are not covered under these laws, and that should change.

Thankfully, there has been some progress on the legal front. California's Attorney General (AG) Kamala Harris brought extortion and identity theft charges against site operators who solicited nude photos and charged hefty fees for their removal.[40] Inspired by AG Harris, the Federal Trade Commission entered into a consent decree with a revenge porn operator for inducing the disclosure of confidential information for financial gain.[41] Also, AG Harris has been working on getting more training for state and local law enforcement.[42] She created a Cyber

38. Amanda Hess, *Why Women Aren't Welcome on the Internet: The Next Frontier of Civil Rights*, PACIFIC STANDARD, Jan. 2014 (Magazine), at 45.

39. CITRON, *supra* note 2, at 23-25.

40. *See generally Attorney General Kamala D. Harris Announces Arrest of Revenge Porn Website Operator*, STATE OF CAL. DEP'T. OF JUSTICE, OFFICE OF THE ATT'Y GEN. (Dec. 10, 2013) https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-arrest-revenge-porn-website-operator (Kevin Bollaert, the operator of UGotPosted, was convicted for engaging in extortion and identity theft.); *see also Attorney General Kamal D. Harris, Tech Leaders and Advocates Launch Offensive in Fight Against Cyber Exploitation*, STATE OF CAL. DEP'T. OF JUSTICE, OFFICE OF THE ATT'Y GEN. (Oct. 14, 2015) https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-tech-leaders-and-advocates-launch-offensive. AG Harris set up a task force to combat the exploitation of networked technologies to disadvantage women and other vulnerable groups, of which I am an adviser.

41. *See* FEDERAL TRADE COMMISSION, WEBSITE OPERATOR IS BANNED FROM REVENGE PORN BUSINESS AFTER FTC CHARGES THAT HE UNFAIRLY POSTED NUDE PHOTOS, (January 29, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/website-operator-banned-revenge-porn-business-after-ftc-charges.

42. *See Attorney General Kamal D. Harris, Tech Leaders and Advocates Launch Offensive in Fight Against Cyber Exploitation*, STATE OF CAL. DEP'T. OF JUSTICE, OFFICE OF THE ATT'Y GEN. (Oct. 14, 2015) https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-tech-leaders-and-advocates-launch-offensive; *see also Governor Signs Second Bill in Attorney General Kamala D. Harris' Cyber Exploitation Legislative Package*, STATE OF CAL. DEP'T. OF JUSTICE, OFFICE OF THE ATT'Y GEN. (Oct. 8, 2015) http://oag.ca.gov/news/press-releases/governor-signs-second-bill-attorney-general-kamala-d-harris%E2%80%99s-cyber-exploitation; *see also* Danielle Citron, *Attorney General Kamala Harris to Help Law Enforcement in Investigations of Criminal Invasions of Sexual Privacy*, LAW ENFORCEMENT CYBER CENTER (Oct. 20, 2015) http://www.iacpcybercenter.org/the-groundbreaking-work-of-attorney-general-kamala-harris-to-help-law-enforcement-in-investigations-of-criminal-invasions-of-sexual-privacy/. In the fall of 2014, I started working with AG Harris and her executive team to help solve this problem. AG Harris put together a Task Force made up of advocates, technology companies like Google, Twitter, Microsoft,

Exploitation Resource Hub,[43] which has a law enforcement bulletin[44] that includes a summary of all of the state (California)[45] and federal laws that can be brought to bear against individuals responsible for posting nude images without consent.[46]

Legislatures have criminalized some forms of revenge porn—more aptly called nonconsensual pornography.[47] In 2005, only New Jersey banned the nonconsensual disclosure of nude images.[48] By 2015, 25 states criminalized the practice.[49] Congresswoman Jackie Speier has drafted a sexual privacy bill that would make revenge porn a federal crime.[50] Federal lawmakers updated the Violence Against Women Act to ensure that the federal cyber stalking statute covered defendants who terrorized victims who lived in the same state.[51] Congresswoman Katherine Clark urged federal authorities to investigate online threats and has proposed a bill that

---

Facebook, and others, and law enforcement representatives. The Task Force worked on many things, including supporting legislation enabling officers to get a warrant for misdemeanors involving nonconsensual pornography, creating tools for law enforcement to use to help them investigate crimes related to nonconsensual pornography, empowering victims to know their rights, and creating best practices for online platforms to follow.

43. *See Cyber Exploitation*, STATE OF CAL. DEP'T. OF JUSTICE, OFFICE OF THE ATT'Y GEN., https://oag.ca.gov/cyberexploitation.

44. *See generally* CAL. DEP'T. OF JUSTICE, DIVISION OF LAW ENFORCEMENT, INFORMATION BULLETIN: ASSISTANCE TO LOCAL LAW ENFORCEMENT AGENCIES IN COMBATTING CYBER EXPLOITATION UNDER NEW AND EXISTING CALIFORNIA LAWS (Oct. 13 2015), http://oag.ca.gov/sites/all/files/agweb/pdfs/ce/cyber-exploitation-law-enforcement-bulletin.pdf?.

45. *Id*.

46. *Id*. *See also* COMMISSION ON PEACE OFFICER STANDARDS AND TRAINING CYBER EXPLOITATION GUIDE FOR LAW ENFORCEMENT, https://www.post.ca.gov/Data/Sites/1/post docs/resources/Cyber Exploitation.pdf (The bulletin highlights the responsibilities of law enforcement agencies in combatting these crimes. In collaboration with California Commission on Peace Officer Standards and Training (POST) and the United States Attorney's office, the Attorney General's office also developed a Commission on Peace Officer Standards and Training (POST) Cyber Exploitation Guide for Law Enforcement.).

47. *See* Cyber Civil Rights Initiative Blog, *supra* note 4.

48. *See generally* N.J. Stat Ann. § 2C14-9 (West 2012).

49. This unusually swift turn of events is thanks in large part to the work of Holly Jacobs's Cyber Civil Rights Initiative and its legislative director Professor Mary Anne Franks who helped draft state laws and the federal revenge porn bill. *See 26 States Have Revenge Porn Laws*, END REVENGE PORN, http://www.endrevengeporn.org/revenge-porn-laws/, (last visited Mar. 7, 2015).

50. *See* Kaveh Waddell, *Bill to Criminalize Revenge Porn Coming After* Recess, NATIONAL JOURNAL (Aug. 12, 2015), https://www.nationaljournal.com/s/70267/bill-criminalize-revenge-porn-coming-after-recess.

51. CITRON, *supra* note 2, at 104.

would secure increased funding to permit federal law enforcement to help provide training to state police in the investigation of cyber harassment cases.[52]

III. THE FIRST AMENDMENT

We can proscribe cyber harassment without undermining free speech values and First Amendment doctrine. The First Amendment does not operate in absolutes. There are certain categories of speech that we can regulate because they contribute so little to cultural and political conversation, and because they cause grave harm.[53]

Cyber harassment often involves categories of speech that enjoy little to no protection. This speech includes true threats, defamation of private individuals about private matters, and crime facilitating speech like extortion, solicitation, and blackmail—those categories of speech enjoy no First Amendment salience or protection.[54] Cyber harassment also involves speech that enjoys less rigorous protection: intentional infliction of emotional distress of private individuals on purely private matters, and the disclosure of private communications about private matters like nude photos. And, cyber harassment involves speech that the Supreme Court understands as conduct—civil rights violations. Civil rights violations can be redressed and punished because they address the interference with victims' life opportunities and the targeting of victims due to group membership.[55]

What of free speech values? An important reason why we protect expression is because it enables us to govern ourselves. To decide the kind of polity we want for ourselves, we have to be able to listen to and talk about ideas—cultural, social, and political. However, cyber harassment contributes nothing to debates necessary for self-governance. What about the importance of speech to the search for truth? Is there something to say about posts suggesting that a victim should be raped or that she wants to

52. *See* Press Release, *Clark Calls for Investigation and Prosecution of Online Threats Against Women*, CONGRESSWOMAN KATHERINE CLARK (Mar. 10, 2015), http://katherineclark.house.gov/index.cfm/press-releases?ID=2CB60BD7-D763-4464-96EB-1D113725559D.

53. U.S. v. Alvarez, 132 S. Ct. 2537, 2550 (2012).

54. *Id*., at 2544. The Court has articulated complex constitutional standards for some of these categories, like defamation, erecting a matrix of fault and damage rules based on whether a plaintiff is a public official or public figure. *See also* Gertz v. Robert Welch, Inc., 418 U.S. 323, 346-349 (1974). As the free speech scholar Rodney Smolla puts it, the well-defined categories of speech falling outside the First Amendment's coverage entail elaborate standards of review, and some constitutional protection is afforded to certain types of libelous speech. Rodney A. Smolla, *Categories, Tiers of Review, and the Roiling Sea of Free Speech Doctrine and Principle: A Methodological Critique of United States v. Alvarez*, 76 Alb. L. Rev. 499-526, 502 (2013).

55. CITRON, *supra* note 2, at 218-220.

have sex with strangers? Only an extreme view of the market place of ideas would view threats, nude images, and defamation as truths worthy of debate. It is true that harassers express themselves as they perpetrate online abuse, but, as Owen Fiss has argued, sometimes we lower the voices of those whose speech silences others.[56] This is especially so when the whole point of harassers' speech is to stop victims' from engaging with the world around them. Victims cannot stay online if they are constantly under sustained assault.

Of course, recognizing victims' expressive interests does not make it any easier to regulate cyber harassment. Our concern for victims' ability to engage online does not, and should not, clear the path for legal claims or prosecutions at odds with our commitment to "uninhibited, robust, and wide open public discourse."[57] Law cannot, and should not, censor hateful or offensive viewpoints.

IV. RESPONSE OF SOCIAL MEDIA COMPANIES

What about online providers who can address cyber harassment without concern about the First Amendment and who enjoy immunity from liability for others' content? Recently, social media companies have been considering if certain abuse is permitted on their platforms.[58] Victims' expressive interests are behind their bans on threats, harassment, and revenge porn.[59] Some companies have attributed their updated policies to the concept of digital citizenship—the various ways networked tools can foster expression and civic engagement.[60]

Consider Twitter's evolving policies. For years, Twitter only required users to refrain from engaging in copyright violations, spam, and impersonations. Its terms-of-service agreement has been expanded to prohibit threats, targeted harassment, and disclosures of private and confidential information (including social security numbers and nude images posted without consent).[61] Twitter's General Counsel attributed the

56. Owen M. Fiss, *Why the State?*, 100 HARV. L. REV. 781, 786 (1987) (stating, "Autonomy may be protected, but only when it enriches public debate").

57. N.Y. Times Co. v. Sullivan, 376 U.S. 254, 301-302 (1964).

58. EMILY BAZELON, STICKS AND STONES: DEFEATING THE CULTURE OF BULLYING AND REDISCOVERING THE POWER OF CHARACTER AND EMPATHY 267 (2014).

59. *See Section 230 of the Communications Decency Act*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/cda230. As private actors that enjoy immunity from liability for the postings of others under Section 230 of the federal Communications Decency Act, content hosts can host as much or as little of their users' speech activities as they wish.

60. Danielle Keats Citron & Helen Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*, 91 B.U. L. Rev. 1435, 1446 (2011).

61. *See* Jessica Gyunn, *Twitter Bans "Revenge Porn"*, USA TODAY (Mar. 12, 2015), http://www.usatoday.com/story/tech/2015/03/12/twitter-bans-revenge-porn/70215684/. See also Amit Singhal, *"Revenge Porn" and Search*, GOOGLE

company's policy changes to its responsibility to "ensure that voices are not silenced because people are afraid to speak up."[62] Users have to "feel safe . . . to fully express themselves."[63] For Twitter, "online safety is a shared responsibility, and digital citizenship is essential to fostering a safe environment for all."[64]

Other providers should consider structuring terms-of-service (TOS) agreements around users' rights and responsibilities, much as Twitter has done.[65] What would this entail? Users would enjoy the right to express themselves on issues large and small. They could contribute to social, cultural, and political dialogue. They could criticize others' views without the fear of private censorship. Such policies would secure the conditions for robust and confident citizenship envisioned by John Stuart Mill and Justice Louis Brandeis.[66] At the same time, users would be barred from using platforms to threaten, harass, and invade sexual privacy. Such behavior "shuts down more expression than it opens up by causing silence, retreat, isolation, or intimidation."[67]

Of course, platforms would need to explain what they mean by the terms threats, targeted harassment, and privacy invasion. Users should be told what happens if their speech violates TOS; they should be given a chance to appeal decisions about their speech. These efforts would help protect the expression of all users.

CONCLUSION

PUBLIC POLICY BLOG (June 19, 2015), http://googlepublicpolicy.blogspot.com/2015/06/revenge-porn-and-search.html and Jacqueline Beauchere, *"Revenge Porn:" Putting Victims Back in Control*, MICROSOFT ON THE ISSUES (July 22, 2015), http://blogs.microsoft.com/on-the-issues/2015/07/22/revenge-porn-putting-victims-back-in-control/. One by one, social media platforms updated their community guidelines to ban revenge porn during 2015. Search engines Google and Microsoft's Bing have pledged to de-index nude images from victims' search results if victims did not consent to their posting.

62. *See* Shreyas Doshi, *Policy and Product Updates Aimed at Combating Abuse*, TWITTER (Blog) (Apr. 21, 2015), https://blog.twitter.com/2015/policy-and-product-updates-aimed-at-combating-abuse.

63. *Id*.

64. *See* Patricia Cartes, *Introducing the New Twitter Safety Center*, TWITTER (Blog) (July 20, 2015), https://blog.twitter.com/2015/introducing-the-new-twitter-safety-center.

65. *Id*.

66. *See* Samuel Warren and Louis Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 219 (1890). *See also* JOHN STUART MILL, ON LIBERTY (1869).

67. *See* Sarah Agudo & Alex Feerst, *We've Been Thinking Hard about How to Create a Medium Where People Treat Each Other Well*, THE STORY, MEDIUM (July 27, 2015), https://medium.com/the-story/we-ve-been-thinking-hard-about-how-to-create-a-medium-where-people-treat-each-other-well-8a62695850cb.

In less than a decade, we have seen meaningful change in the law and its enforcement. We have seen private companies respond to the plight of cyber harassment victims. We have seen bravery and activism that has helped change the social meaning of cyber harassment. Holly Jacobs founded the Cyber Civil Rights Initiative to help others faced with online harassment. Anita Sarkeesian has spent considerable time speaking out against online abuse, earning her TIME's Top 100 recognition. Now is the time to talk about cyber harassment and to recognize how far we have come and how far we need to go.