CYBER CIVIL RIGHTS: LOOKING FORWARD

DANIELLE KEATS CITRON†

The *Cyber Civil Rights* conference raised so many important questions about the practical and normative value of seeing online harassment as a discrimination problem. In these remarks, I highlight and address two important issues that must be tackled before moving forward with a cyber civil rights agenda.[1] The first concerns the practical—whether we, in fact, have useful antidiscrimination tools at the state and federal level and, if not, how we might conceive of new ones. The second involves the normative—whether we should invoke technological solutions, such as traceability anonymity, as part of a cyber civil rights agenda given their potential risks.

As Helen Norton underscored at the conference, current federal and state antidiscrimination law can move the cyber civil rights agenda forward, but only so far. On the criminal side, the Civil Rights Act of 1968 does indeed punish "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.[2] Courts have sustained convictions of defendants who made threats over employees' email and voicemail.[3] A court upheld the prosecution of a defendant who left messages on an Arab American's voice mail that threatened "the only good Arab is a dead Arab." Similarly, a jury convicted a defendant for sending an email under the name "Asian Hater" to 60 Asian students that read: "I personally will make it my life career [sic] to find and kill everyone of you personally."[4]

Crucially, however, federal criminal law does not extend to threats made because of a victim's gender or sexual orientation. This must change, particularly because victims of online threats are predominantly chosen due to their gender or sexual orientation.[5] So how might legisla-

---

† Professor of Law, University of Maryland School of Law. I am ever grateful to Professor Viva Moffat, Mike Nelson, and Jake Spratt for conceiving and orchestrating the *Cyber Civil Rights* conference. Their insights and those of our panelists will have an indelible mark on my future work on the subject.

1. There are naturally many more weaknesses, though I concentrate on these two, which struck an important chord for the participants at the conference.

2. 18 U.S.C. 245(b)(2)(C) (2006).

3. *E.g.*, United States v. Syring, 522 F. Supp. 2d 125 (D.D.C. 2007).

4. PARTNERS AGAINST HATE, INVESTIGATING HATE CRIMES ON THE INTERNET: TECHNICAL ASSISTANCE BRIEF 5 (2003).

5. *See* Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 378–79 (2009) (explaining that over 60% of online harassment victims are women and that when perpetrators target men for online harassment, it is often because the victims are believed to be gay).

tors do that? Current law could be amended to criminalize online threats made because of a victim's gender or sexual orientation. The *Violence Against Women Act* (VAWA) might be a profitable place to begin this effort. Although the Supreme Court struck down VAWA's regulation of gender-motivated violence on the grounds that such criminal conduct did not substantially affect interstate commerce to warrant congressional action under the Commerce Clause, Congress could amend VAWA pursuant to its power to regulate an instrumentality of interstate commerce—the Internet—to punish anonymous posters who threaten individuals because of their gender or sexual orientation. Such a legislative move would surely find support from the Department of Justice, which encourages federal prosecutors to seek hate crime penalty enhancements for defendants who subject victims to cyber harassment because of their race, color, religion, national origin, or sexual orientation.[6]

This leaves us to examine antidiscrimination actions for civil remedies. Much like the criminal side, the civil law side permits private lawsuits for discriminatory actions taken because of a victim's race. For instance, § 1981of Title 42 of the U.S. Code guarantees members of racial minorities "the same right in every State . . . to make and enforce contracts . . . as is enjoyed by white citizens." Section 1981 permits lawsuits against private individuals without the need for state action because Congress enacted the statute under its power to enforce the Thirteenth Amendment.[7] Courts have allowed plaintiffs to bring § 1981 claims against masked mobs that used tactics of intimidation to prevent members of racial minorities from "making a living" in their chosen field.[8]

Here, again, individuals have limited means to sue defendants who seek to prevent them from making a living online due to their gender or sexual orientation. In *Cyber Civil Rights*, I argued that women might bring claims against attackers under Title VII of the Civil Rights Act of 1964 because just after the statute's passage, courts upheld discrimination claims where masked defendants engaged in intimidation tactics to prevent plaintiffs from pursuing their chosen careers. Yet, as I acknowledged there and as Norton emphasized at the conference, Title VII decisions now overwhelmingly focus on employer-employee relationships, rendering my suggestion one that courts will not lightly adopt.

One way to address this serious problem is to urge Congress to amend Title VII to permit individuals to sue defendants who interfere with individuals' online work because of their gender or sexual orientation. Although doing so would, in part, honor Title VII's broader goal of

---

6. PARTNERS AGAINST HATE, *supra* note 4, at 5.

7. To that end, courts have interpreted religious groups, such as Jews, as a race protected by the Thirteenth Amendment. *See, e.g.*, United States v. Nelson 277 F.3d 164 (2d Cir. 2002).

8. Vietnamese Fishermen's Ass'n v. Knights of the Ku Klux Klan, 518 F. Supp. 993 (S.D. Tex. 1981).

eliminating discrimination in women's employment opportunities, pressing for Congressional change is a daunting task. Indeed, one might say it would be Sisyphian.[9] Advocates might pursue change in state legislatures even though their contributions would naturally be more limited. This is something that my future work will explore in earnest.

Now for the unintended, and potentially destructive, consequences of technological solutions to implement a cyber civil rights agenda. In *Cyber Civil Rights*, I suggested that an orderly articulation of the standard of care for ISPs and website operators should include a requirement that website operators configure their sites to collect and retain visitors' IP addresses. Such traceable anonymity would allow posters to comment anonymously to the outside world but permit their identity to be traced in the event that they engage in unlawful behavior.[10]

As Paul Ohm and Wendy Seltzer forcefully argued, we should be wary of technical solutions, like traceable anonymity, given the potential for misuse. Ohm argued that once we mandate IP retention to advance a cyber civil rights agenda, those IP addresses might become available to companies seeking to enforce copyright violations against students and accessible to countries seeking the identity of dissidents. In Ohm's words, demanding traceable anonymity is like using Napalm when a surgical strike is available. Seltzer developed the problem with technological optimism by pointing to anti-porn filtering software, which more often than not blocked innocent sites and thus hampered expression on the Internet, and anti-circumvention requirements in copyright, which impaired innovation without stopping the robust pirated DVD market.

Ohm's and Seltzer's arguments are important. Channeling law through technology has an important role but perhaps not in this way. I supported traceable anonymity as a means to protect law's deterrent power. Website operators are so often immune from liability due to § 230 of the Communications Decency Act,[11] leaving only the perpetrators

---

9. I take this notion of a Sisyphean struggle from Deborah Rhode, who so eloquently captured this point when she described women's struggles to combat sexual abuses in the workplace. Deborah L. Rhode, *Sexual Harassment*, 65 S. CAL. L. REV. 1459, 1460 (1992). She explained that women's struggles have "elements of a feminist myth of Sisyphus" because many women are still pushing the same rock up the hill with regard to occupational segregation, stratification, and subordination. *Id.* The enforcement of the law of sexual harassment "reflects a commitment more to equality in form than equality in fact." *Id.*

10. I also argued that courts should release the names of posters to plaintiffs *only* if plaintiffs could provide proof that their claims would survive a motion for summary judgment. This would assure posters of the safety of their anonymity in the face of baseless allegations.

11. Even under the broad interpretation of § 230, website operators can be sued if they explicitly induce third parties to express illegal preferences. In 2008, the Ninth Circuit addressed whether Roommates.com enjoyed § 230 immunity for asking posters questions about sex, sexual orientation, and whether the person has children as part of the sign up process. Plaintiffs argued that those questions, if asked offline, could violate Fair Housing laws. The Ninth Circuit found that defendant lacked immunity under CDA because it created the questions and choice of answers and thus was the "information content provider" as to the questions and in turn the answers that it required. The court reasoned that the CDA does not grant immunity for inducing third parties to express illegal prefer-

to pursue for legal remedies and prosecutions. In other words, a cyber civil rights agenda may have limited coercive and expressive power unless perpetrators see that the costs of their conduct exceed the benefits.

There are, of course, other ways to address this problem aside from traceable anonymity. One possibility is a variation of a notice and takedown regime. Law could require website operators to retain a poster's IP address only after receiving notice of legitimate claims of illegal or tortious activity. Of course, this regime could be manipulated by individuals who aim to identify an individual based on frivolous claims. It would raise other negative externalities as well, such as chilling concerns. This is just one of many possible ways to address the inability to identify cyber harassers. Nonetheless, thinking of alternatives to traceable anonymity seems an indispensable part of the future of a cyber civil rights agenda.

---

ences. Eric Goldman expertly addressed the implications of the Roommates.com case at the conference.