CYBER-EXPLOITATION AND DISTRIBUTED ENFORCEMENT

JANE R. BAMBAUER & DEREK E. BAMBAUER*

Many thanks to Danielle Citron and to the Law Review for inviting us to comment on her important and thought-provoking book, *Hate Crimes in Cyberspace*. To us, the most striking finding in the book is that we lack not laws but law enforcement. In many cases, victims meet with indifference from police or prosecutors, despite clear-cut evidence of crime. Statutory prohibitions on Internet stalking, harassment, revenge porn, and other violations provide little benefit if they lie unused. Successful enforcement actions are sufficiently rare to warrant significant media attention. Part of Citron's solution is to shift perceptions and norms around these types of cyberspace attacks, using workplace sexual harassment as a model. This is valuable work, but it has a relatively long time horizon.

In the near term, at least, we advocate for greater distributed enforcement, through measures such as tort claims and copyright litigation. If victims are given better tools to identify and bring claims against their harassers, a small subset who are willing to do so can perform effective work as "private attorneys general."[1] Such efforts can punish their individual harassers and deter the harassers of many others. Private actions theoretically should be an attractive part of the solution to the problems that Citron identifies, since they place blame and costs on the most culpable individuals. Such efforts, though, must grapple with the inevitable trade-off between privacy and personal security.[2] We argue here that facilitating private litigation is worth its privacy costs. If it isn't, that finding is enlightening in itself—if the most direct forms of legal accountability are hampered by countervailing policy considerations, the indirect forms will be even more challenging.

First, consider the benefits of private actions. Tort claims provide a valuable model for how distributed enforcement against cyber-exploitation might work. First, torts benefit from a long common law history of evolution and adaptation, making them familiar and flexible for judges. Indeed, Citron's own work looks

* Associate Professor and Professor of Law, University of Arizona James E. Rogers College of Law. The authors welcome comments at <janebambauer@email.arizona.edu> and <derekbambauer@email.arizona.edu>.

[1] Assoc. Indus. v. Ickes, 134 F.2d 694, 704 (2d Cir. 1943).

[2] On the distinction between the two, see Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667 (2013).

to tort law to solve information-based harms.[3] Plaintiffs have drawn upon tort to deal with challenges unique to the information age, such as spam,[4] Web site scraping by bots,[5] and identity theft.[6] Second, tort law includes limiting principles that help ensure liability attaches only for serious harms[7] and that protect freedom of expression.[8] Those features operate to police the dividing line between hate speech and hate crimes, ensuring that protected speech is not chilled. Third, tort law authorizes punitive damages for malicious or willful unlawful conduct. Punitive damages deter effectively by offsetting (at least partially) the risk of underdetection.[9] And, they increase the victim's potential recovery, which makes her case more attractive to plaintiffs' lawyers. While federal law shields intermediaries from liability,[10] tort claims empower victims to go after those who have violated their rights regardless of whether law enforcement or prosecutors see the case as worth their time.

Similarly, copyright law is principally enforced by private parties. And, because copyright remedies include injunctive relief and operate against third parties,[11] it is particularly potent as a tool for attacking the unauthorized release of intimate media, including revenge porn. As much as 80% of revenge porn images are selfies, enabling victims to file take-down notifications with Internet platforms, sue intermediaries that ignore the notices, and enjoin violators from re-distributing the pictures.[12] In some cases, victims will be able to obtain

[3] 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 (2007).

[4] CompuServe v. Cyber Promotions, 962 F. Supp. 1015 (S.D. Ohio 1997).

[5] Register.com v. Verio, 356 F.3d 393 (2d Cir. 2004).

[6] Doe v. Friendfinder Network, 540 F. Supp. 2d 288 (D.N.H. 2008).

[7] For example, the tort of Intentional Infliction of Emotional Distress, which can cover a wide range of harassing behavior that does not fit nicely into the elements of other intentional torts, requires "severe" distress caused by "outrageous" conduct. RESTATEMENT (SECOND) OF TORTS § 46 (1965). Although the standard for outrageous conduct is variable and unpredictable, it is supposed to go well beyond garden variety slights and mean-spirited behavior that people inevitably experience in the social world. Daniel Givelber, The Right to Minimum Social Decency and the Limits of Evenhandedness: Intentional Infliction of Emotional Distress by Outrageous Conduct, 82 COLUM. L. REV. 42 (1982).

[8] *See, e.g.*, Roberts v. Saylor, 230 Kan. 289, 293 (Kan. 1981) ("It should be understood that liability does not arise from mere insults, indignities, threats, annoyances, petty expressions, or other trivialities."). However, at times, the Supreme Court has had to rein in tort law when state court interpretations have run afoul of constitutional protections for free speech. See Hustler Magazine v. Falwell, 485 U.S. 46 (1988); N.Y. Times v. Sullivan, 376 U.S. 254 (1964).

[9] A. Mitchell Polinsky & Steven Shavell, *Punitive Damages: An Economic Analysis*, 111 HARV. L. REV. 869, 874-875 (1998).

[10] 47 U.S.C. § 230.

[11] 17 U.S.C. §§ 502(a), 512(j).

[12] See Amanda Levendowski, *Using Copyright to Combat Revenge Porn*, 3 N.Y.U. J. INTELL. PROP. & ENT. L. 422 (2014).

statutory damages for successful copyright infringement claims, creating deterrence and increasing access to counsel.[13] Copyright is an underrated tool in the arsenal for combatting cyber-exploitation.

Citron urges Web site operators to design for better, more civil interactions among users. Web sites that are designed for accountability of their users will also assist harassment victims who decide to bring private actions against their tormenters. But these changes to Web sites have privacy implications that Citron and others might find unpalatable.[14] To police user-generated content effectively, sites will have to focus on users, not just the material they post. Anonymous comment threads are the bane of the Internet, and on pseudonymous sites, users easily bounce among names and identities. Banning trolls requires knowing some information about them—an IP address, e-mail address, Facebook log-in, or the like. That data helps both sites and users impose consequences for bad behavior: blocking a particular account from posting, downvoting their comments, and initiating litigation. Trolls can be more easily banished back under their bridges and hence may be less likely to crawl out in the first place.

However, measures that make users more identifiable apply to travelers and trolls equally. Privacy advocates worry about the aggregation of personally identifiable information, the use of that data to engage in activities such as targeted advertising, and the ability of governments to access those details. For good and ill, designing sites or applications to enhance identity-driven consequences links a user—or at least information that can lead to him—to his content. That is helpful when it unmasks someone vile on Reddit. It is worrisome when the information is used to track Black Lives Matter protesters on behalf of police. Retaining this identifying information over time can be useful in spotting users who switch names or accounts. But, if enough data is kept, it can turn into one of the reservoirs of danger that Citron highlights in earlier work, exemplified by the data breaches at the Office of Personnel Management, Anthem, and Experian. Private sector abuses of personal information worry us less than governmental misuse. Storing this data makes it accessible to the state, often with far less process or justification than the probable cause that would support a warrant.[15] While some firms are trying to mitigate this problem through transparency measures such as warrant canaries, those methods are crude at best—they do not help an individual user assess her risks in using the site.

Thus, architectural decisions present us with hard choices. Tor enables both dissidents and pedophiles to exchange information free from surveillance. Yelp's requirement to register before posting deters overblown reviews, but also

[13] 17 U.S.C. § 412.

[14] Data collection on Web users may later become accessible to the government or be part of an algorithmic scoring system. David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013); Danielle Keats Citron & Frank Pasquale, *The Scored Society*, 89 WASH. L. REV. 1 (2014).

[15] Jane Bambauer, Other People's Papers, 94 TEX. L. REV. __ (forthcoming 2015).

leaves consumers with negative experiences vulnerable to lawsuits from aggrieved businesses. Building sites that reduce cyber-exploitation comes at a cost that we ought to acknowledge. Indeed, our proposals here to use private, distributed enforcement depend in part on access to some identifying information to be effective. While some architectural changes can be effective without accumulating data on identifiable users, tort and copyright solutions unquestionably rely on the victims' ability to identify their perpetrators, conjuring up all the trade-off described above.

Danielle Citron's book both generates and marks an important shift in the discussion over cyber-exploitation on-line. We seek to enrich that debate by focusing on the potential for robust self-help through distributed legal enforcement, and by pointing up the hard choices that architectural changes require.