

BREAKING FELTEN'S THIRD LAW: HOW NOT TO FIX THE INTERNET

PAUL OHM[†]

I applaud the *Denver University Law Review* for organizing a symposium around the Cyber Civil Rights work of Danielle Citron, because she deserves great credit for shining a light on the intolerable harms being inflicted on women every day on online message boards.¹ Professor Citron (along with Professor Ann Bartow²) has convinced me of the importance of the Cyber Civil Rights movement; we urgently need to find solutions to punish and deter online harassers, to allow the harassed to use the Internet without fear.

But although I embrace the goals of the movement, I worry about some of the solutions being proposed in the name of Cyber Civil Rights. Professor Citron, for example, has suggested mandatory logfile data retention for website providers.³ Suggestions like these remind me of something I have heard Professor Ed Felten say on many occasions: “In technology policy debates, lawyers put too much faith in technical solutions, while technologists put too much faith in legal solutions.” This observation so directly hits its mark, I feel compelled to give it a name: Felten’s Third Law.⁴ For solving problems, lawyers look to technology, and techies look to law.

As we try to achieve the goals of the Cyber Civil Rights movement, we should break Felten’s Third Law. We lawyers and law professors should seek legal and not technical solutions to attack online harassment. It is better to try to increase the odds of civil liability and criminal prosecution than it is to mandate data retention or order the redesign of systems. This, I argue, is the lesson of recent history. The problem of online harassment echoes Internet problems that have come before. Ever since the masses started colonizing the Internet in the mid-1990’s, successive

[†] Associate Professor, University of Colorado Law School. I thank Viva Moffat, Mike Nelson, and Jake Spratt of the University of Denver Sturm College of Law for inviting me to the symposium.

1. Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U.L. REV. 61 (2009); Danielle Keats Citron, *Law’s Expressive Value in Combatting Cyber Gender Harassment*, 108 MICH. L. REV. 373 (2009).

2. Ann Bartow, *Internet Defamation as Profit Center: The Monetization of Online Harassment*, 32 HARV. J.L. & GENDER 383 (2009).

3. Citron, *Cyber Civil Rights*, *supra* note 1, at 123 (describing a standard of care called “traceable anonymity” which would “require website operators to configure their sites to collect and retain visitors’ IP address”). At the symposium, Professor Citron remarked that she has begun to rethink her call for mandatory data retention.

4. I’m not sure what Ed Felten’s first two laws are, but because he has said so many wise things, I am hedging my bets by calling this his third law.

waves of people have been troubled by different kinds of online speech and conduct and have tried to restructure both law and technology in response.

There is a nice temporal rhythm revealed here, because these crusades have happened to ebb and flow with the close and dawn of decades; the 1990's was the decade of pornography and the Aughts was the decade of copyright infringement. In case the 2010's becomes the decade of Cyber Civil Rights, we should look to the histories of porn and copyright infringement for guidance.

In the 1990's, many worried about the problem of porn, and in particular, worried that children could easily access porn intended only for adults. The movement was spurred, at least in part, by a law review article, one now notorious for its poorly executed empirical research.⁵ This article spurred not only a cover story in Time Magazine,⁶ but also action in Congress. Citing the research on the Senate Floor, Senator Grassley introduced a bill, the Protection of Children from Computer Pornography Act of 1995. Although this bill did not pass, it paved the way for a series of troublesome, ill-conceived laws that followed.

In 1996 Congress enacted the Communications Decency Act ("CDA"),⁷ which sought broadly to prohibit the posting of "indecent" material on the Internet. In 1999, the Supreme Court struck down the indecency ban in the landmark First Amendment and Internet case, *Reno v. ACLU*.⁸ In response, Congress enacted the Child Online Protection Act,⁹ which like the CDA was quickly enjoined and eventually put to its final death just last year.¹⁰ The legal responses to online porn were sweeping, unconstitutional, and after the courts were finished ruling, mostly harmless.

Not only did anti-porn crusaders look to law, but also they turned to technology and in particular, to Internet filtering software. Many of them had hoped that Internet filters would step in where the law had failed by technologically preventing access to porn online. Many companies and researchers tried to make Internet filters easier to use, harder to circumvent, and more accurate. Policymakers tried to force filters onto computers and networks, and in 2000, Congress enacted the Children's Internet

5. Martin Rimm, *Marketing Pornography on the Information Superhighway*, 83 GEO. L.J. 1849 (1995). The Rimm study was widely criticized. For an example of the criticism, see Donna L. Hoffman & Thomas P. Novak, A Detailed Analysis of the Conceptual, Logical, and Methodological Flaws in the Article: "Marketing Pornography on the Information Superhighway," July 2, 1995 (version 1.01), available at http://w2.eff.org/Censorship/Rimm_CMU_Time/rimm_hoffman_novak_critique.

6. Philip Elmer-Dewitt, *Cyberporn*, TIME, July 3, 1995.

7. Pub. L. No. 104-104, 110 Stat. 56 § 502 (Feb. 8, 1996).

8. 521 U.S. 844 (1997).

9. Pub. L. 105-277, § 1403, 112 Stat. 2681-736 (Oct. 21, 1998).

10. *ACLU v. Mukasey*, 534 F.3d 181 (3d Cir. 2008), *cert. denied*, 129 S. Ct. 1032 (2009).

Protection Act (“CIPA”),¹¹ which mandates Internet filtering for indecent material on computers in public schools and libraries, a law that is still on the books.

This is the first historical marker: The 1990’s, the decade of first legal and then technical solutions to stamp out Internet porn. But just as this crusade began to run out of steam, the next great online struggle emerged. In June 1999, as Congress began writing CIPA, teenager Sean Fanning released Napster, the first Internet-wide peer-to-peer (“p2p”) system designed specifically for trading music files.

As their anti-porn crusading counterparts had done before them, the recording industry has engaged in both legal and technical campaigns against p2p copyright infringement. First, it filed lawsuits. In December 1999, the Recording Industry Association of America (“RIAA”) sued Napster. This was only the first in a series, as it sued many others who created p2p software and ran p2p networks. Steadily, the recording industry won a series of court victories, in the process expanding interpretations of copyright law, culminating in the landmark case, *MGM v. Grokster*, which held that p2p companies Grokster and Streamcast could be held liable for inducing their users to infringe copyrights.¹²

Evidently unsatisfied by these victories against providers, in 2003, the industry embraced another strategy: suits against the file traders themselves. This aggressive campaign seems to have been at least a qualified success: countless have been threatened, tens of thousands have been sued, and at least two have been found liable by juries. At the very least, the lawsuits seem to be informing p2p users that their actions may have consequences, at least judging from what I have seen in the press, blogs, and in my classrooms.

But like the anti-porn crusaders before them, the anti-p2p copyright warriors have turned to technical fixes as well as lawsuits. Most importantly, the RIAA has searched for ways to deal with online pseudonymity. Because our actions online are attached to IP addresses but not directly to identities, those who want to stamp out speech or conduct online need to find a way to pierce pseudonymity. The recording industry attacked Internet pseudonymity in the courts, seeking and often winning rulings imposing only low hurdles to unmasking. But they also began searching for non-legal solutions, which they still are searching for today. To my mind, this is the most problematic phase of the p2p copyright war.

The RIAA seems to want to re-architect the Internet to make pseudonymity much harder to obtain. For example, it has been arguing for three strikes laws which would require ISPs to kick off the Internet any

11. Pub. L. No. 106-554, 114 Stat. 2763A-335 (Dec. 21, 2000).

12. 545 U.S. 913 (2005).

users who are accused—not proved guilty, merely accused—of copyright infringement three times. In addition, the RIAA seems to be pressuring ISPs to detect and maybe block copyrighted content traveling across the Internet.¹³

* * *

I've hummed a few bars of history to explain why, when I hear Cyber Civil Rights advocates calling for technical fixes, I feel as if I've heard the song before. To be sure, the Cyber Civil Rights movement differs in important ways from the anti-porn crusades of the 90's and the anti-p2p wars of the Aughts: Most obviously, the harms described by scholars like Professor Citron are fundamentally and meaningfully different from the purported harms in these other skirmishes. The subjugation and terrorization of women Professor Citron describes is a much more significant problem than the problems of porn or copyright infringement online, at least according to the best arguments I have seen for each.

But once we move past harms to solutions, we can spot many similarities and learn many lessons. In past campaigns to squelch problematic categories of Internet speech, legal solutions have ranged from the scary-but-never-implemented (CDA) to the quixotic and wasteful but mostly harmless (RIAA lawsuits). The trend suggests that so long as the Cyber Civil Rights movement focuses on legal solutions—on bringing lawsuits against harassers, encouraging criminal prosecutions of the worst offenders, and in rare cases, actions against message board operators who benefit from the harassment—it might find workable solutions without doing too much harm.

In contrast, technical solutions too often lead to unintended consequences. Anyone who has ever struggled to use a computer with an Internet filter, cursing at the false positives and giggling at the false negatives, can breathe a sigh of relief that the anti-porn crusaders never convinced anyone to place filters deep inside the network itself. Likewise, we should worry about the recording industry's plans for ISP filtering and three strikes laws as overbroad, disproportionate measures.

If anything, technical solutions may be even less likely to succeed against the problem of online harassment than in the earlier battles. Music and porn travel through the Internet as large files, which can be easy to identify through fingerprinting and filtering. In contrast, Cyber Civil Rights harms often involve threats and harassment buried in small snippets of text whose threatening nature must be judged by a person not a machine. For all of these reasons, we should be deploying surgical strikes, not napalm.

13. Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417.

In particular, I am most concerned about calls to increase identifiability and decrease pseudonymity, such as calls for mandatory data retention. I have many problems with these proposals, based in concerns about overdeterrence, chilling effects, and threats to the fundamental nature of the Internet. For now, let's focus on only one problem, the Hermit Crab Problem. You build this beautiful structure, it does a very good job providing you the shelter and food you need, but you wake up one morning and find that some other creature has moved into it.

If it were to become harder to hide on the Internet, not only would this make it easier to out Cyber Civil Rights harms, but also it would become easier to stamp out any type of disfavored Internet speech. It's what I have heard Deirdre Mulligan call The Fully-Identified Internet Problem. If the Cyber Civil Rights movement ever brings a fully-identified Internet proposal to Congress, the copyright warriors will be sitting in a back row of the hearing room, quietly cheering them on. Across the room, the anti-porn crusaders will be doing the same. Others will be there too, such as those who dislike dissidents and whistleblowers. We can't empower only one of these groups without empowering them all.

Forget technical solutions. Build a Cyber Civil Rights movement, and use it to propose solutions to the problems of online hate and harassment, but focus those solutions on the narrow, surgical tools afforded by law, including many of the creative legal proposals presented elsewhere in this symposium.