Networks of Empathy

Thomas E. Kadri

*University of Georgia School of Law*

Follow this and additional works at: [https://dc.law.utah.edu/ulr](https://dc.law.utah.edu/ulr)

Part of the Communications Law Commons, and the Computer Law Commons

**Recommended Citation**


This Article is brought to you for free and open access by Utah Law Digital Commons. It has been accepted for inclusion in Utah Law Review by an authorized editor of Utah Law Digital Commons. For more information, please contact [valeri.craigle@law.utah.edu](mailto:valeri.craigle@law.utah.edu).
NETWORKS OF EMPATHY

Thomas E. Kadri

Abstract

Digital abuse is on the rise. People increasingly use technology to perpetrate and exacerbate abusive conduct like stalking and harassment, manipulating digital tools to control and harm their victims. By some accounts, 95% of domestic-abuse cases involve technology, while a sizeable chunk of the U.S. population now admits to having suffered or perpetrated serious abuse online. To make matters worse, people often trivialize digital abuse or underestimate its prevalence. Even among those who do appreciate its severity, there remains ample disagreement about how to address it.

Although law can be a powerful tool to regulate digital abuse, legal responses are by no means the only option. This Essay explores how both computer code and social norms can prevent and mitigate forms of digital abuse that aren’t easily addressed through law. These regulatory responses should be grounded in empathy for victims of digital abuse. Empathy demands imaginatively putting oneself in a victim’s place and attempting to feel as they feel—a trying task made easier by heeding victims’ stories. We can neither understand nor address digital abuse unless we view technology in a deeper social context and grapple with how and why digital abuse is harmful. This Essay urges key figures to exhibit greater empathy in developing code and norms to help victims, proposing ways that technologists, police officers, educators, employers, and victims can use these extralegal means to combat an increasingly pervasive form of abuse.

© 2020 Thomas E. Kadri. Assistant Professor, University of Georgia School of Law; Mellon Fellow, Yale Law School. I’m indebted to Danielle Citron and Mary Anne Franks for their leadership in this field, as well as their feedback on this Essay. Reading their work has been inspiring and therapeutic. I also wish to thank Jack Balkin, Monica Bell, Jenny Carroll, Harlan Cohen, Ellen Cosgrove, Jennifer Czinčz, Adam Dodge, Evelyn Douek, Melissa Durkee, Luiza Ferreira Lima, Sarah Haan, Mark Lemley, Mason Marks, Ali Miller, Przemek Palka, Robert Post, Mathias Reimann, Neil Richards, Alan Rozenshtein, Clare Ryan, Liron Shilo, Olivier Sylvain, Jacob Victor, Ari Waldman, Diego Werneck Arguelhes, and Andrew Keane Woods for thoughtful conversations or comments, and Emily Nuvan and Kayla Race for excellent editing. Lastly, for their tireless care, I dedicate this Essay to Natália Pires de Vasconcelos, Ross Harris, and Tony Senanayake, and to the friends who supported me but who would rather remain nameless.
INTRODUCTION

People are worried about technology’s role in disinformation, and rightly so. When lies spread online, it becomes hard to distinguish what’s true from what’s false. But as we grapple with how technology fuels political deceit, let’s not forget that similar tools are also being exploited for intimate purposes.1 Our democracy is important, but we shouldn’t succumb to “politico-centrism” by “overstress[ing] the importance of politics to the life of ordinary citizens.”2 The technologies enabling people to deceive for political gain also empower people to stalk, harass, surveil, and oppress.3 Digital technologies are powerful, and we shouldn’t be surprised that their power can be wielded for negative as well as positive ends, for private as well as political purposes.

Digital abuse is on the rise.4 People increasingly use technology to perpetrate and exacerbate abusive conduct, relying on digital tools to exert power over others.

---

1 Danielle Citron, for example, warns of politically catastrophic “deep fakes” but reminds us that 98% of these digital manipulations are “deep fake sex videos.” Brian Feldman, MacArthur Genius Danielle Citron on Deepfakes and the Representative Katie Hill Scandal, INTELLIGENCER (Oct. 31, 2019), http://nymag.com/intelligencer/2019/10/danielle-citron-on-the-danger-of-deepfakes-and-revenge-porn.html [https://perma.cc/A6Q4-4QKZ].


4 I use the term “digital abuse” to capture a broad range of abusive conduct enabled by technology. The term covers not only the ways that people use technology to engage in conduct typically prohibited by stalking and harassment laws but also newer means of surveillance, privacy invasions, and threats that increasingly occur in contemporary domestic abuse (such as sharing nonconsensual pornography or monitoring a person’s online activity without permission). See, e.g., GA. CODE ANN. § 16-11-39.1(a)(1) (2020) (defining the offense of “harassing communications” as when a person “[c]ontacts another person repeatedly via telecommunication, e-mail, text messaging, or any other form of electronic
Sometimes the perpetrators are strangers, sometimes they’re familiar, but always they’re manipulating technology to control and harm their victims.\(^5\)

Looking to Lawrence Lessig’s regulatory quartet, we might try to stem this surge of digital abuse through law, markets, computer code, or norms.\(^6\) Law can do much good, but legislators have been skittish about regulating technology for fear of interrupting innovation or reaching unconstitutional dead ends.\(^7\) Market forces

communication for the purpose of harassing, molesting, threatening, or intimidating such person or the family of such person”); GA. CODE ANN. § 16-5-90(a)(1) (defining the offense of “stalking” as when a person ("follows, places under surveillance, or contacts another person at or about a place or places without the consent of the other person for the purpose of harassing and intimidating the other person"); YBARRA ET AL., supra note 3, at 9 (presenting a taxonomy of digital abuse that includes posting “nearly nude or nude photos or videos . . . online without [a person’s] permission”). For an excellent summary and analysis of the types of abusive conduct (beyond stalking and harassment) that I have in mind, see YBARRA ET AL., supra note 3, at 3–4, 9–18.

\(^5\) See Danielle Keats Citron, Cyber Mobs, Disinformation, and Death Videos: The Internet as It Is (and as It Should Be), 118 MICH. L. REV. 1073 (2020) [hereinafter Citron, Cyber Mobs].

\(^6\) See LAWRENCE LESSIG, CODE VERSION 2.0 121–27 (2006); see also WILLIAM J. MITCHELL, CITY OF BITS: SPACE, PLACE, AND THE INFOBahn 111 (1995) (describing computer code as “law” in cyberspace); Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules Through Technology, 76 TEX. L. REV. 553, 554–55 (1998) (discussing how law isn’t “the only source of rulemaking” in networked environments because “[t]echnological capabilities and system design choices impose rules on participants”). Lessig’s work explores how these four forces—law, markets, code, and norms—can regulate behavior in cyberspace. Laws like copyright and defamation regulate our ability to speak online, while norms in various online communities might also constrain what we say. LESSIG, supra, at 124. Markets, too, affect our behavior online, such as when pricing structures restrict access. Id. Lastly, computer code creates the “architecture” of cyberspace, shaping our experiences online in diverse ways by making some actions possible and others impossible. Id. at 124–25. My focus on Lessig’s framework follows Danielle Citron’s pathbreaking work, which has long championed a multifaceted approach that looks beyond purely legal interventions to combat digital abuse. See, e.g., DANIELLE CITRON, HATE CRIMES IN CYBERSPACE 226–50 (2014) [hereinafter CITRON, HATE CRIMES] (discussing ways that technology companies, parents, and schools can “shift online norms” surrounding digital abuse); Danielle Keats Citron, Spying Inc., 72 WASH. & LEE L. REV. 1243, 1252–53, 1273–80 (2015) [hereinafter Citron, Spying] (outlining how we might “improve the law, its enforcement, and other non-legal efforts” to address technologies that enable cyberstalking).

should do more, but many of the economic incentives appear more likely to hinder than help the fight against digital abuse.\footnote{See Siva Vaidhyanathan, Antisocial Media: How Facebook Disconnects Us and Undermines Democracy 5–20 (2018).}

What of code and norms? This Essay explores how these extralegal forces are increasingly essential in tackling digital abuse, especially forms of abuse that aren’t easily regulated by law.\footnote{See Mark A. Lemley & Eugene Volokh, Law, Virtual Reality, and Augmented Reality, 166 U. PA. L. REV. 1051, 1075 (2018) (arguing that code is “maybe the most effective sort of law” to respond to some new technologies).} There’s an urgent need to adjust technical architecture and change social customs to address how people are using technology to inflict serious harm on others. But we can’t begin to face this challenge without understanding how digital abuse actually affects victims. This Essay therefore argues that regulatory responses to digital abuse should be grounded in empathy.

A comprehensive response to harm relies on empathy. By placing ourselves in another’s shoes, by wrestling with their experiences and feelings, we can better understand and respond to their suffering.\footnote{Adam Smith, The Theory of Moral Sentiments 9 (D.D. Raphael & A.L. Macfie eds., Liberty Fund ed. 1982, photo. reprint Oxford Univ. Press 1976) (“By the imagination we place ourselves in his situation, we conceive ourselves enduring all the same torments, we enter as it were into his body, and become in some measure the same person with him, and thence form some idea of his sensations, and even feel something which, though weaker in degree, is not altogether unlike them.”).} This “fellow-feeling,” to use Adam Smith’s term, rests on imagination.\footnote{Id. at 10. Smith refers to this quality as “sympathy,” but modern scholars largely agree that he’s describing contemporary conceptions of empathy. See, e.g., Ken Binmore, Natural Justice 115 (2005); James A. Vela-McConnell, Who Is My Neighbor?: Social Affinity in a Modern World 118 (1999); Mary Anne Franks, How to Feel Like a Woman, or Why Punishment Is a Drag, 61 UCLA L. REV. 566, 594 (2014) [hereinafter Franks, How to Feel Like a Woman]. Though Smith’s dominant focus was on empathy for another’s suffering, he did not confine himself to that emotion. Smith, supra note 10, at 10.} When we engage our imaginations, we can go beyond feeling sympathy for another’s suffering and conceive of that suffering as part of our own experience.\footnote{Id. at 20–21 (“My companion does not naturally look upon the misfortune that has befallen me, or the injury that has been done me, from the same point of view in which I consider them.”).} This act of imagination requires work, for empathy doesn’t always come naturally.\footnote{Id. at 21; see also David Hume, A Treatise of Human Nature 319 (L.A. Selby-Bigge ed., Oxford Univ. Press 1960) (1739).} But, with effort, a person can achieve that “imaginary change of situation” from which empathy derives.\footnote{See SIVA VAIDHYANATHAN, ANTIMEDIA: HOW FACEBOOK DISCONNECTS US AND UNDERMINES DEMOCRACY 5–20 (2018).}
Mere sympathy for victims is inadequate because it allows people to maintain distance from the harms caused by digital abuse. Feeling sorrow or pity is a start, but extralegal regulatory efforts should involve people imaginatively putting themselves in a victim’s place and attempting to feel as they would feel.15 As Mary Anne Franks has explained, “[s]ympathy maintains the divide between the observer of suffering and the observed; empathy attempts to dissolve it.”16 In this sense, “[e]mpathy allows us to free ourselves from the limitations of our own self-interest, whereas sympathy is merely coextensive with self-interest.”17 To truly undermine digital abuse, we should employ empathy.

Empathetic responses to digital abuse should harness the regulatory power of code and norms. It’s easy to say abstractly that technology companies should design their products in ways likely to mitigate digital abuse. But code isn’t organic—people write it—and if we want empathetic technology, we must be more conscious about the people who create it. Code-based efforts will miss the mark if technologists lack awareness about digital abuse and fail to empathize with victims. Those charged with designing products should appreciate the severity of digital abuse—why a

---

15 See Franks, How to Feel Like a Woman, supra note 11, at 594. The word “empathy” is a translation of the German word “einfühlung,” coined by Robert Vischer in 1873. See Magdalena Nowak, The Complicated History of Einfühlung, 1 ARGUMENT 301, 304–05 (2011). Vischer sought to explain a person’s feeling of similarity and harmony with a work of art—an “entry” into the work, enabled by a person’s imagination, that creates an “empathic relationship with the object.” Id. at 305. Theodore Lipps then built on Vischer’s work to capture how people experience a similar sense of connection with other humans before Edward Titchener brought the word into the English language as “empathy” in 1907. See Theodor Lipps, Ästhetik: Psychologie des Schönen und der Kunst (Vol. 1) (1903); Edward B. Titchener, Lectures on the Experimental Psychology of the Thought-Processes (1909). There’s plenty of disagreement about how best to define empathy, especially the comparative definitions of sympathy and empathy. See Franks, How to Feel Like a Woman, supra note 11, at 593–94; Douglas Chismar, Empathy and Sympathy: The Important Difference, 22 J. VALUE INQUIRY 257 (1988); Stephen Darwall, Empathy, Sympathy, Care, 89 PHILO. STUD. 261 (1998); Philippe Fontaine, Identification and Economic Behavior: Sympathy and Empathy in Historical Perspective, 13 ECON. & PHILOS. 261 (1997); Heidi L. Maibom, Feeling for Others: Empathy, Sympathy, and Morality, 52 INQUIRY 483 (2009); Lauren Wispé, The Distinction Between Sympathy and Empathy: To Call Forth a Concept, a Word Is Needed, 50 J. PERSONALITY & SOC. PSYCHOL. 314 (1986). For my part, I follow Mary Anne Franks’s lead and take sympathy to mean “the capacity to feel sorrow or pity for another person,” whereas empathy describes “the capacity to imaginatively put oneself in the place of another and attempt to feel as they feel.” Franks, How to Feel Like a Woman, supra note 11, at 594.


17 Franks, How to Feel Like a Woman, supra note 11, at 594.
response is needed—and the many modes of abuse—how and why it happens—and for that they need empathy for victims. Still, better technology won’t fix everything; as Danielle Citron reminds us, human beings are often “the bug in the code.”

So we must also try to deter digital abuse and alleviate its harms by shifting norms. To do this, we must first raise awareness about digital abuse. Education efforts should resist pernicious stereotypes and build empathy across the gender spectrum, preferably through institutional support in places of work and education.

In part, this Essay aspires to enhance our capacity to imagine how digital abuse affects victims and mobilize people to confront the harms increasingly enabled by technology. I argue that storytelling can be a powerful vehicle to engender empathy. Whether it’s through victims being employed at technology companies, product designers consulting with victims before launching new products, police and educators receiving training informed by victims’ experiences, or even academics giving victims a voice through their scholarship, I believe that victims’ stories should be heard, grappled with, and understood with a view toward promoting empathy.

I’m by no means the first person to recommend using code and norms to regulate digital abuse, nor is it novel to argue that harms perpetrated digitally are serious. This Essay seeks to build on these past efforts and provoke more thinking in this space. I hope to make three main contributions. First, I urge key figures to make empathy for victims an animating principle in responding to digital abuse. Second, I explore how victims’ stories can raise awareness about the realities of digital abuse in ways that lead to more empathetic coding and norms. Finally, I suggest specific ways that technologists, police officers, educators, employers, and victims can use extralegal means to combat this devastating and widespread form of abuse.

I divide this Essay in two Parts. Part I focuses on code, exploring how technologists should embrace empathetic design to tackle digital abuse but concluding that technical interventions can take us only so far. Part II therefore advocates using social norms to deter digital abuse and lessen its harms, arguing that

---


19 Franks, How to Feel Like a Woman, supra note 11, at 593 (arguing that “the tolerance of sexual abuse of both women and men is accomplished in large part by a failure of imagination, and hence of empathy”).

20 See infra Section II.A.

21 Danielle Citron, in particular, has advocated for a comprehensive approach to addressing digital abuse—one that recognizes how law is an important but not exclusive part of the regulatory toolkit. See supra note 6.

22 One need only read Julian Dibbell’s 1993 masterpiece, A Rape in Cyberspace, to know that people have long being making such claims. See Julian Dibbell, A Rape in Cyberspace, VILLAGE VOICE (Dec. 23, 1993), https://www.villagevoice.com/2005/10/18/a-rape-in-cyberspace [https://perma.cc/P434-AVUE].
we should raise awareness and challenge the regressive stereotypes that inhibit empathy for victims.

I. CODE-BASED RESPONSES TO DIGITAL ABUSE

Digital abuse is rife. A recent study found that 18% of internet users have experienced serious online threats, harassment, and stalking. A domestic-violence charity, Refuge, estimates that 95% of its abuse cases involve technology, while the National Domestic Violence Hotline saw a 155% increase in reports of digital abuse between 2015 and 2018 as other forms of abuse remained fairly constant. According to another poll, one in ten Americans admits to using “stalkerware” apps to siphon information and images from their partner’s or ex’s phone. “People think this problem is niche, but that’s not true,” reports Rahul Chatterjee, a computer scientist who studies digital abuse. After all, one in three women and one in six men have experienced abusive relationships, constituting millions of people in the United States alone. Given how central digital devices have become in daily life, it’s predictable that technology will play a role in domestic abuse.

---


27 Jee, supra note 24.

28 Id.
To compound the problem, people often underestimate the gravity of digital abuse. Victims’ lives are disrupted and damaged. Their health suffers. Their work is jeopardized. Their relationships deteriorate. Their safety is threatened. Their domestic and professional stability crumbles. Their communities grieve. Abusers use technology to “create a sense of being ever-present in the victim’s life.” This incessant attack is exhausting and debilitating. Not only do victims spend hours worrying about their physical and emotional wellbeing, but documenting their abuse for the police can become a full-time job. Even if the abuse eventually subsides, the effects can endure long after. Many victims end up suffering from post-traumatic stress disorder.

Trivialization is a longstanding and stubborn societal problem, both for harassment generally and digital abuse specifically. This is especially true with respect to harms disproportionately suffered by women. As Danielle Citron laments, “[s]ociety ignored or downplayed domestic violence’s brutality for over 200 years,” and “[n]o term even existed to describe sexual harassment in the workplace until the 1970s, despite the pervasiveness of the practice.” Danielle Keats Citron, Law’s Expressive Value in Combating Cyber Gender Harassment, 108 Mich. L. Rev. 373, 376 (2009) [hereinafter Citron, Law’s Expressive Value]; see also id. at 392–404 (tracing historical trivialization of women’s suffering, from sexual assault to domestic violence to workplace harassment and now to cyber-harassment).

Eric Blaauw et al., The Toll of Stalking: The Relationship Between Features of Stalking and Psychopathology of Victims, 17 J. INTERPERSONAL VIOLENCE 50, 57–58 (2002) (finding that stalking victims suffer much higher rates of depression, anxiety, insomnia, and social dysfunction than the general population); Ari Ezra Waldman, Amplifying Abuse: The Fusion of Cyberharassment and Discrimination, 95 B.U. L. REV. ANNEX 83, 83 (2015) (“Cyberharassment devastates its victims. Anxiety, panic attacks, and fear are common effects; post-traumatic stress disorder, anorexia and bulimia, and clinical depression are common diagnoses.”).

Mary Anne Franks, Sexual Harassment 2.0, 71 Md. L. Rev. 655, 658 (2012) [hereinafter Franks, Sexual Harassment].

Mary Anne Franks, “Not Where Bodies Live”: The Abstraction of Internet Expression, in FREE SPEECH IN THE DIGITAL AGE 137, 140 (Susan J. Brison & Katharine Gelber eds., 2019) [hereinafter Franks, “Not Where Bodies Live”].


See Waldman, supra note 30, at 83 (arguing that the “personal effects” of digital abuse “are part of a larger social cancer that breeds sexism, subjugation, and inequality”).

stress disorder,\textsuperscript{37} others resort to self-protective isolation and silence because they fear their abuser will reemerge the moment they raise their head above the parapet.\textsuperscript{38}

If technology is part of the problem, it might also be part of the solution. Scholars have long touted technological design as an antidote to technological ills, proposing that systems be built conscientiously.\textsuperscript{39} But as Neil Richards has noted, “[t]echnological innovation is not magical, nor is it contained to the mythic realm of ‘cyberspace,’ which is no more or less profound than what it is at bottom—people using technology, sometimes for good, sometimes for evil, and most of the time for something in between.”\textsuperscript{40} If we want to tackle digital abuse through code, we should think carefully about the people who create it.\textsuperscript{41}

\textit{A. Cultivating Better Code}

Improving code can make a big difference in thwarting digital abuse.\textsuperscript{42} Design choices make technologies more or less “regulable” because some architectures enable greater behavioral control than others.\textsuperscript{43} Technologists know this, yet design flaws plague the industry. These flaws are often thoughtless, not malicious, but carelessness should be no excuse. Communication technologies aren’t “neutral” or

\textsuperscript{37} See Michele Pathé & Paul E. Mullen, \textit{The Impact of Stalkers on Their Victims}, 170 BRIT. J. PSYCHIATRY 12, 14 (1997) (finding that 37\% of stalking victims fulfill the diagnostic criteria for post-traumatic stress disorder).


\textsuperscript{40} Neil M. Richards, \textit{The Internet Grows Up?}, 95 B.U. L. REV. ANNEX 33, 35 (2015).

\textsuperscript{41} See Olivier Sylvain, \textit{Recovering Tech’s Humanity}, 119 COLUM. L. REV. F. 252, 252 (2019) (encouraging focus on the “indispensable role that human managers at the Big Tech companies have in developing and selecting their business designs, algorithms, and operational techniques”).


\textsuperscript{43} Lessig, \textit{supra} note 6, at 24; see also Lemley & Volokh, \textit{supra} note 9, at 1070–87 (discussing how certain criminal and harmful behavior in virtual environments might be easier to regulate through code than law).
“empty” vessels, but instead present particular “constraints and opportunities” for people who use them. At every step along the way, technologists should mull over how a particular tool might be used and abused, and they should insert safety valves to foil potential abusers. In short, social networks should be designed empathetically, not cavalierly.

Consider Facebook’s “People You May Know” feature, which recommends new connections based on the company’s secret-sauce algorithms. Although finding long-lost friends might seem benign and even beneficial, the tool has a darker—albeit unintentional—side. A woman went out on a date with a man who began harassing her when she spurned his advances. Although the woman never gave him her real name, a year later he tracked her down on Facebook after the platform unmasked her as one of the “people he may know.” As Kashmir Hill observed in reporting the story, “[w]hen you start aggressively mining people’s social networks, it’s easy to surface people we know that we don’t want to know.” Nobody at Facebook intended to advertise victims to their abusers, but the company surely failed to code empathetically.

An empathetic technologist might have anticipated Facebook’s “algorithmic cruelty.” It reminds me of a similar feature on Microsoft Outlook’s phone

---

46 Google, for example, uses code to inhibit stalkers from tracking their victims’ locations. When a person’s location is shared with a third party through Google Maps, the platform sends out warning messages at unpredictable intervals to thwart stalkers who might sporadically have access to the victims’ phone. Andy Greenberg, The Simple Way Apple and Google Let Domestic Abusers Stalk Victims, WIRED (July 2, 2019, 10:50 AM), https://www.wired.com/story/common-apps-domestic-abusers-stalk-victims [https://perma.cc/JME6-GW4S].
48 Id.
49 Id. The feature also began suggesting connections between sex workers and their clients, revealing the real names of people who have safety concerns about being publicly exposed. Kashmir Hill, How Facebook Outs Sex Workers, GIZMODO (Oct. 11, 2017, 02:20 PM), https://gizmodo.com/how-facebook-outs-sex-workers-1818861596 [https://perma.cc/QZH4-NUN7].
application, which lists “suggested” contacts on its homepage to make it easier to reach the people who frequently contact you. No doubt this coding makes many people’s lives slightly easier. For victims, though, it might show them their abuser’s name every single day. Even after a victim blocks a person who floods their phone with emails and calls, that person’s name might still appear on Outlook’s list for months because of the sheer volume of overall contact. When I reached out to Microsoft to suggest that they allow people to remove unwanted names, the company thanked me for suggesting such a “great feature” to add in future versions. Although this response can be applauded as empathetic, it also suggests that Microsoft’s engineers could have avoided this flawed coding on the front end had they fully considered the dynamics of digital abuse. (I’ll note, too, that Microsoft doesn’t seem to have rolled out my “great feature” quite yet.)

Cultivating empathetic perspectives within the industry is essential to avoid this kind of technological myopia. To encourage greater empathy, technology companies should draw from people who have the experiences and perspectives conducive to understanding digital abuse. This involves hiring abuse victims, for whom the comprehension comes naturally, albeit painfully. Technology companies should also staff diversely throughout departments. Everyone from engineers to policymakers should be ensconced in a range of perspectives, especially from marginalized people who traditionally face higher levels of online mistreatment. For those lacking background experiences likely to foster empathy for victims, companies should offer training to increase awareness about digital abuse. Finally, companies should consult externally with experts and victims.

240 [https://perma.cc/WRB3-PS78]; see also generally Anthony T. Pinter et al., “Am I Never Going to Be Free of All This Crap?” Upsetting Encounters with Algorithmically Curated Content About Ex-Partners, 3 Proc. ACM Hum.-Comput. Interaction 70:1 (2019) (explaining the results of an empirical study that examined how Facebook’s algorithms oversimplify people’s social lives and present them with upsetting and insensitive content).


52 SARA WACHTER-BOETTCHER, TECHNICALLY WRONG: SEXIST APPS, BIASED ALGORITHMS, AND OTHER THREATS OF TOXIC TECH 13–26 (2017) (discussing various problems linked to the lack of diversity at many technology companies).


54 See also infra Part II (discussing the need and means to raise awareness about digital abuse).

55 Twitter, for example, has the good sense to consult regularly with Danielle Citron on issues of digital abuse, while TikTok has recently enlisted the expertise of Mary Anne Franks. See The Twitter Trust and Safety Council, Twitter, https://about.twitter.com/en_us
Some people might think this advice outdated. They might have the sense that diversity in the tech industry has already improved significantly, but this impression seems to be illusory. The gender gap, for example, persists in staggering rates. According to one 2017 study, 90% of U.S. start-up founders are male, and 82% of start-up teams are entirely male. The divide endures beyond fledgling tech companies; remarkably, there’s only one woman to every 3.76 men employed at the “Big 5” tech companies (Amazon, Facebook, Apple, Google, and Microsoft).

Racial diversity is also a major concern, with an estimated 77.1% of venture-backed start-up founders being white and only 1.8% being Latino and 1% being black. These figures don’t bode well for creating teams equipped to empathize with victims of digital abuse. After all, ample evidence suggests that women, racial minorities, and sexual minorities face disproportionately high levels of online mistreatment.

Technology companies should do more to hire, fire, train, and consult with an eye toward breeding empathy for victims. Beyond hiring diversely, technology companies can also make structural efforts to encourage all of their employees to design empathetically. Just as companies have started to embrace “Privacy by Design,” they could also adopt what we might call


56 RATEMYINVESTOR, DIVERSITY IN U.S. STARTUPS 7, 12 (2017), https://ratemyinvestor.com/diversity_report [https://perma.cc/2VRA-YSSZ]; see also Jacqueline Ryan Vickery, This Isn’t New: Gender, Publics, and the Internet, in MEDIATING MISOGYNY: GENDER, TECHNOLOGY, AND HARASSMENT 31, 35 (Jacqueline Ryan Vickery & Tracy Everbach eds., 2018) (highlighting a 2012 report that only 25% of computing jobs were held by women and 95% of tech start-ups were owned by men); Franks, Justice, supra note 45, at 1393–96 (discussing “hidden biases” of Wikipedia moderators who are overwhelmingly male).

57 RATEMYINVESTOR, supra note 56, at 7.

58 Id. at 8.

59 See Danielle Keats Citron, Cyber Civil Rights, 89 B.U. L. Rev. 61, 85 (2009) [hereinafter Citron, Cyber Civil Rights] (discussing how “online mobs typically focus on women, people of color, and other traditionally subjugated groups”); see also infra Section II.B.

60 It would be inappropriate for employers to ask potential or current employees whether they have been victims of abuse, but that doesn’t stop technology companies from publicizing their hopes to hire and consult with victims and encouraging victims to come forward if they wish. Companies could also reach out to victims who’ve already publicly disclosed their abuse, so long as any entreaties were made empathetically. I’m grateful to Emily Nuvan for encouraging me to consider this practical point.

61 NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 181 (2015) (discussing how companies could adopt “Privacy by Design” to build privacy protections into their products). For superb treatment of the relationship between privacy and design, see generally WOODROW HARTZOG, PRIVACY’S BLUEPRINT:
Empathy by Design, whereby employees at every level are encouraged to consider how their projects might affect actual or potential victims of digital abuse. Some designers talk about “realizing empathy” to describe the process of going from not empathizing to empathizing. See TEDx Talks, How Empathy Fuels the Creative Process: Seung Chan Lim (Slim) at TEDxWellesleyCollege, YouTube (Apr. 1, 2014), https://youtu.be/CGLUzYUKhT5 [https://perma.cc/F98Q-RBLQ]. Others draw on psychology literature to discuss different forms of empathy and ways to bring empathy into design processes. See, e.g., Indi Young, Practical Empathy: For Collaboration and Creativity in Your Work 24–25, 34–35 (2015); Daniel Goleman, What Is Empathy?, in Emotional Intelligence: Empathy 1, 4–9 (Harvard Bus. Review ed., 2017) (distinguishing between cognitive empathy, emotional empathy, and empathic concern); Indi Young, Practical Empathy, Presentation at UX Lausanne (May 23, 2014) (transcript available at https://indiyoung.com/conference-presentation-practical-empathy [https://perma.cc/XM7D-AK9C]) (discussing the differences between emotional and cognitive empathy); O’Reilly, A Practical Type of Empathy - Indi Young Keynote, YouTube (May 30, 2015), https://www.youtube.com/watch?v=TSs0iB6gxV4&t=1s [https://perma.cc/Q9AN-R6E8] (discussing how cognitive empathy is more “viable” than emotional empathy as a way to implement empathy within a company or design process). And some have proposed detailed processes that companies can follow to develop an “empathetic design process” that shifts “from an external focus on the market, or an internal focus on technology, to an empathetic focus on people.” See Jon Kolko, A Process for Empathetic Product Design, in Emotional Intelligence: Empathy 71, 73–76, 80 (Harvard Bus. Review ed., 2017).

62 Some designers talk about “realizing empathy” to describe the process of going from not empathizing to empathizing. See TEDx Talks, How Empathy Fuels the Creative Process: Seung Chan Lim (Slim) at TEDxWellesleyCollege, YouTube (Apr. 1, 2014), https://youtu.be/CGLUzYUKhT5 [https://perma.cc/F98Q-RBLQ]. Others draw on psychology literature to discuss different forms of empathy and ways to bring empathy into design processes. See, e.g., Indi Young, Practical Empathy: For Collaboration and Creativity in Your Work 24–25, 34–35 (2015); Daniel Goleman, What Is Empathy?, in Emotional Intelligence: Empathy 1, 4–9 (Harvard Bus. Review ed., 2017) (distinguishing between cognitive empathy, emotional empathy, and empathic concern); Indi Young, Practical Empathy, Presentation at UX Lausanne (May 23, 2014) (transcript available at https://indiyoung.com/conference-presentation-practical-empathy [https://perma.cc/XM7D-AK9C]) (discussing the differences between emotional and cognitive empathy); O’Reilly, A Practical Type of Empathy - Indi Young Keynote, YouTube (May 30, 2015), https://www.youtube.com/watch?v=TSs0iB6gxV4&t=1s [https://perma.cc/Q9AN-R6E8] (discussing how cognitive empathy is more “viable” than emotional empathy as a way to implement empathy within a company or design process). And some have proposed detailed processes that companies can follow to develop an “empathetic design process” that shifts “from an external focus on the market, or an internal focus on technology, to an empathetic focus on people.” See Jon Kolko, A Process for Empathetic Product Design, in Emotional Intelligence: Empathy 71, 73–76, 80 (Harvard Bus. Review ed., 2017).

63 See Wachter-Boettcher, supra note 52, at 27 (explaining how companies “use tools called personas—fictional representations of people who fit their target audiences—when designing their products, apps, websites, and marketing campaigns”).

64 Id. at 38–41, 74–75; see also Libby Bawcombe, Designing New Products with Empathy: 50 Stress Cases to Consider, Design at NPR (Aug. 16, 2016), https://npr.design/designing-news-products-with-empathy-50-stresscases-to-consider-61f068a939eb [https://perma.cc/7DKU-8FHX] (“Stress cases help us design for real user journeys that fall outside of our ideal circumstances and assumptions.”).

65 Bawcombe, supra note 64.

66 Id.
on the outskirts, not only producing a better product but also helping those who need it most.

There will be times, of course, when designing empathetically is costly. We might doubt, then, that technology companies will make empathetic choices that interfere with their profit-maximizing corporate responsibilities. This skepticism represents a serious objection, though there were likely similar concerns about many privacy and security features that aren’t legally mandated but have nonetheless found their way into technological design. Companies will generally have considerable wiggle room to serve both shareholders’ and victims’ interests. And when they don’t, we might use it as a canary-in-the-coal-mine moment to convince legislators that new laws are needed.

The bigger struggle will be persuading technology companies to take victims’ interests seriously. There are various sources of leverage that can encourage empathetic design. A starting point is identifying ways that designing empathetically can be lucrative, perhaps because the design will create goodwill and help to retain a company’s customers or because it will entice more people (including victims) to start using their products. When the numbers don’t support these arguments, governments can create better financial incentives by funding programs that promote empathetic design. The National Science Foundation, for example, recently ran a competition to award federal funding for pressing research questions, and one finalist pitched the idea of “Promoting Empathy-Based AI” by suggesting that technologists working on Artificial Intelligence should pursue progress “in a way that promotes empathy and compassion in the world.” States, international organizations, and private foundations could offer similar rewards for empathetic initiatives. And no matter the financial considerations, we can always rely on the coercive force of bad press when technology companies enable digital abuse. This approach—which echoes how privacy advocates highlight data breaches to promote privacy-protective design choices—presumes that technologists are likelier to exhibit greater empathy for victims if the realities of digital abuse are publicly exposed, especially if their companies are seen as complicit.

---


70 See Greenberg, supra note 46 (discussing the interplay between journalistic and academic exposés about digital abuse and technology companies’ design responses).
A final pressure point on companies might come from their corporate peers. This motivation could build on initiatives by transnational constituencies to encourage the private sector to safeguard human rights, or it could come from within the tech industry itself—especially if shareholder activists rally around the cause. In the wake of various scandals and misdeeds, shareholder activists have created investor organizations to hold technology companies accountable, demand better practices, and set benchmarks for corporate performance. These investor organizations have already started pushing companies to be more conscious of certain types of digital abuse, and others could urge technologists to embrace empathy throughout the design process.

To be sure, there’s good reason to be cynical about technology companies’ incentives to behave empathetically absent legal mandates to protect victims from digital abuse. There will surely be companies that aren’t stirred by any of the sources of leverage outlined above. But there’s at least some evidence that at least some companies will be motivated at least some of the time, and that’s a start. Extralegal regulation must always reckon with enforcement challenges because it lacks the state’s coercive power, but imperfection doesn’t mean impotence.

If a technology company is willing to embrace empathetic design in theory, the (perhaps literally) million-dollar question is what this means in practice. Although each technology has peculiar needs, a few general considerations should guide a company’s coders and policymakers. To begin with, users should have more choices and more control. Abuse dynamics vary greatly, so a one-size-fits-all approach will usually fall short. Take blocking—an essential tool to help victims curtail abuse. “Users can be blocked at various levels, ranging from being unable to share, tag, and upvote other’s posts, to being fully unable to access any aspect of content associated with their profile.”

---


73 See, e.g., id. at 57 (discussing the efforts of one organization to establish a set of “Tech Expectations for Combating Child Sex Exploitation Online”).

74 See Lemley & Volokh, supra note 9, at 1087–91 (arguing that greater optionality can address various forms of harmful or offensive behavior in virtual-reality environments).

75 danah boyd, Dear Voyeur, Meet Flâneur . . . Sincerely, Social Media, 8 SURVEILLANCE & SOC’Y 505, 505 (2011) (observing that “technology brings the flâneur and the voyeur together in new ways,” affecting our comfort at being watched and watching others).
with another user’s profile. Some services, however, offer one-dimensional blocking tools: a person is either blocked or unblocked with fixed boundaries. On Twitter, for example, a blocked user will still appear in your feed when other users reply to their tweets or mention them. Some victims will be fine with seeing their abuser’s name in this context; others won’t. Empathetic design would give people the choice.

Technologists should also experiment with what Danielle Citron calls anti-abuse “counterspeech.” Though we might usually think of counterspeech as confronting falsehoods with truth, we can repurpose the term to capture expression by technology companies that seeks to deter digital abuse. Think, for instance, about technologies like “tracking pixels” that help abusers monitor their victims by email. A sender can insert these pixels into an email to discover information about the recipient, including when and even where the emails are opened. Advertisers use this technology to conduct market research, but abusers also use it to stalk their victims. Not only might abusers use these pixels to discover sensitive information, but this kind of digital surveillance can deter victims from reporting harassment for fear of antagonizing an abuser who could be alerted when a tracked email is forwarded to the police.

How might code-based counterspeech help here? Although I’d prefer email providers to block this tracking technology altogether through code, they could at least try to dissuade abusers from using it. Some providers allow people to stop the pixels from loading when you open a tracked email, but this does little to alter

---


77 Blocking seems particularly suited to greater optionality. When your abuser is part of your community, as is often the case, you might decide it’s worth seeing online posts engaging with that person for fear of missing conversations involving people in your professional or social circles, but you might also believe the triggering effects aren’t worth the cost.

78 CITRON, HATE CRIMES, supra note 6, at 241.


80 Brian Merchant, How Email Open Tracking Quietly Took over the Web: You Give Up More Privacy than You Might Think Each Time You Open an Email, WIRED (Dec. 11, 2017, 07:00 AM), https://www.wired.com/story/how-email-open-tracking-quietly-took-over-the-web [https://perma.cc/Y5P8-BYKP].

81 Cf. Megan Lindsay Brown et al., Technology-Based Abuse: Intimate Partner Violence and the Use of Information Communication Technologies, in MEDIATING MISOGyny: GENDER, TECHNOLOGY, AND HARASSMENT 209, 216 (Jacqueline Ryan Vickery & Tracy Everbach eds., 2018) (discussing software like “sniffers” that gather information about victims’ email communications).

82 What Is a Tracking Pixel and Can Strangers Really Spy on Me Through Email?: Everything You Need to Know About the Invisible E-mail Tool that Tracks You, VERGE (July
people’s incentives to insert the pixels in the first place. To create greater deterrence, Gmail could, for example, include its own message atop infected emails to warn explicitly that tracking software is revealing the recipient’s location, instead of the bland “Images are not displayed” banner it currently uses. Outlook does slightly better, declaring that “some pictures in this message were not downloaded” to “protect your privacy,” but this opaque language still fails to capture the extent of intrusion and surveillance facilitated by tracking pixels. Many victims are likely surveilled for much longer because they’re simply unaware. Counterspeech could at least provide them with better notice.

Lastly, a company’s computer code should conform to a corporate ethical code. If taken seriously, company values can determine which product ideas sink or swim. Strong values can also guard against “technological determinism”—a Silicon Valley virus that assumes “society should conform itself to the dictates of technology rather than the other way around.” Companies considering new features should ask critical normative questions: “Who reaps its benefits? What values are embedded in its design? . . . Should it exist at all?” Google, for instance, refuses to serve advertisements for abuse-related searches. Others should mimic similar stances.

Facebook’s story offers cautionary tales. Mark Zuckerberg’s early mantra—“Move fast and break things”—captures the kind of reckless ethically that allows digital abuse to flourish. Even Facebook’s later slogan—“Making the world more open and connected”—is a normatively questionable maxim. The phrase appears to be a descriptive statement about what the company aspires to do, but the nestled assumption is that achieving this goal is desirable. The benefits of greater openness and connection are contestable, and Facebook’s naivety on this issue reflects the


83 See Jee, supra note 24.

84 Franks, Justice, supra note 45, at 1380; see also Richards, supra note 40, at 35 (discussing importance of “ensur[ing] that our cherished values are faithfully translated into digitally-mediated formats”).

85 Franks, Justice, supra note 45, at 1382 (emphasis added); see also Jee, supra note 24 (discussing how Google and Apple might adopt standards, vetting processes, and checklists to bar unethical stalkerware apps from their devices).


fantasy of technological utopia” that cultivates digital abuse on many online platforms. To give Facebook a little credit, the company has become somewhat more transparent about its values, giving the public a smidgen of soft power to hold it accountable for failing to live up to its own morals. But having known values doesn’t mean having good values. In a worrying move, Facebook quietly discarded “equality” and “equity” from its enumerated values, replacing them with the ambiguous principle of “authenticity.” The company’s embrace of external supervision through a new Oversight Board has some promise, but only if the body establishes itself as a persuasive force that holds Facebook accountable. At the very least, the Board should openly explain Facebook’s policies and flesh out what the company’s buzzword values actually mean. Only then can we judge and understand them.

Oversight mustn’t stop with external boards. Companies should permit outside researchers to study how their technologies enable digital abuse. Many technology companies are reluctant to allow external research, sealing themselves off as gatekeepers that withhold access to the information necessary to expose problems with their products. Although some excellent research exists in this area, much

---

89 See Franks, Justice, supra note 45, at 1397.
93 See Citron, Hate Crimes, supra note 6, at 231 (discussing the value of technology companies openly explaining their policies); Rory Van Loo, Federal Rules of Platform Procedure, U. Chi. L. REV. (forthcoming 2021) (manuscript at 1, 29–30) (on file with author) (arguing that platform oversight boards should issue public decisions and develop transparent precedents to inform their users because online platforms behave as private courthouses).
94 See Thomas E. Kadri, Digital Gatekeepers, 99 Texas L. Rev. (forthcoming 2021) (critiquing cyber-trespass laws like the federal Computer Fraud and Abuse Act that give
work remains to understand this ever-evolving terrain. Companies can’t be trusted to police themselves if we’re to monitor digital abuse.

B. Resisting Technochauvinism

Taking steps to cultivate empathetic code is essential. Ultimately, though, we mustn’t be lulled into “technochauvinism,” or “the belief that tech is always the solution.” As Woody Hartzog and Evan Selinger advise, “design strategies aren’t magical techno-fixes.” Code gets us only so far.

For one thing, many abusers use technologies that are unlikely to change, usually because society values the benefits they bring. Karen Levy has explored how digital abuse is often “mundane” in that it requires “little to no sophistication” and relies on “everyday devices and services.” Abuse by email is perhaps the clearest

online platforms gatekeeper rights to block external research); Thomas E. Kadri, Platforms as Blackacres, 68 UCLA L. REV. (forthcoming 2021) (outlining possible First Amendment challenges to using cyber-trespass laws to shield online platforms from external scrutiny).


96 MEREDITH BROUSSARD, ARTIFICIAL UNINTELLIGENCE: HOW COMPUTERS MISUNDERSTAND THE WORLD 7–8 (2018); see also EVGENY MOROZOV, TO SAVE EVERYTHING, CLICK HERE: THE FOLLY OF TECHNOLOGICAL SOLUTIONISM 5–9 (2014) (criticizing the ideology of “solutionism,” which mistakenly views technology as the answer to all sorts of problems); Evgeny Morozov, The Tech ‘Solutions’ for Coronavirus Take the Surveillance State to the Next Level, GUARDIAN (Apr. 15, 2020, 10:46 AM), https://www.theguardian.com/commentisfree/2020/apr/15/tech-coronavirus-surveillance-state-digital-disrupt (discussing how “[s]olutionists deploy technology to avoid politics” by arguing that “the best we can do is to apply digital plasters” to solve problems, including the coronavirus pandemic). Given the tech industry’s diversity deficiency, Broussard’s term can serve as an unintentional double entendre, reminding us to resist technochauvinism by being conscious about the gender dynamics of code and coding. See discussion supra notes 56–59 and accompanying text.

97 Hartzog & Selinger, supra note 76, at 51.

There are certainly salutary reasons why people might seek anonymity online. See Citron, Hate Crimes, supra note 6, at 238–39; danah boyd, The Politics of “Real Names”: Power, example.\textsuperscript{99} Society derives huge value from easy-to-create email services that are free and accessible to all, but abusers can effortlessly create pseudonymous accounts to evade blocking and impersonate other people. When victims repeatedly receive emails from new accounts, they might feel as if they can never escape their abuse. Email is essential—you can’t simply opt out—and starting afresh with a new account can carry huge social costs. But as long as a victim keeps the same email address, they can be relentlessly contacted through new accounts that dodge other technical barriers they erect.\textsuperscript{100}

In other instances, changing code might inadvertently harm victims because the same technology used to abuse victims can help to protect them.\textsuperscript{101} Although phone-enabled abuse is rampant, smartphones can be liberating and privacy-enhancing devices,\textsuperscript{102} allowing victims to gather proof of abusive messages and calls, forward evidence to the police, and communicate with support networks when they feel in danger. Screenshooting, in particular, can be invaluable. Calls don’t appear on phone records unless they’re answered—something that many victims hate doing and that the police often discourage. But without evidence of repeated contact from an abuser, victims are unlikely to get legal protection, so one option is to take screenshots of call activity and forward them to the police—an exhausting but beneficial practice. On balance, many victims will be thankful for their phones even when the technology becomes a conduit for abuse.

Perhaps the biggest reason not to put too much faith in code is that some technologists are unwilling to redesign particular products empathetically, and all it takes is one holdout. Take spoofing services, which allow people to make calls and send messages displaying numbers that aren’t theirs; or masking services, which hide identifying information on Caller ID.\textsuperscript{103} Spoofing services provide an especially

\textsuperscript{99} See Pew Study 2014, supra note 23, at 5–6 (finding that 16% of people reported that their most recent experience of digital abuse occurred through a personal email account).

\textsuperscript{100} Similar concerns arise with devices like pre-paid phones, which can be purchased easily and without identification. No doubt they increase accessibility for people who can’t afford regular phone plans or who need immediate access to a phone in an emergency. But these devices—and the lack of records that they generate—have made abuse too simple, allowing abusers to evade blocking measures by repeatedly purchasing new numbers. See Cindy Southworth & Sarah Tucker, Technology, Stalking and Domestic Violence Victims, 76 Miss. L.J. 667, 674 (2007). Even when a judge issues a subpoena to unmask the person who purchased the phone, it’s often impossible to trace the user’s identity. See id.

\textsuperscript{101} See Brown et al., supra note 81, at 221 (discussing how technologies can be a “lifeline” for victims of abuse); Southworth & Tucker, supra note 100, at 667 (asserting that “victims of domestic violence are using the revolutionary tool of the Internet to map roads to new lives by reaching out to shelters, researching restraining orders, and finding housing and employment opportunities”).

\textsuperscript{102} See Jo Tacchi et al., Meaningful Mobility: Gender, Development and Mobile Phones, 12 Feminist Media Studies 528, 531 (2012).

\textsuperscript{103} There’s been longstanding debate about the costs of technology-enabled anonymity. There are certainly salutary reasons why people might seek anonymity online. See Citron, Hate Crimes, supra note 6, at 238–39; danah boyd, The Politics of “Real Names”: Power,
easy way to prolong and exacerbate abuse, both digital and physical. By pretending to be someone close to the victim, abusers can trick the victim into answering unwanted calls or messages, causing them to lower their guard and divulge sensitive information. Some abusers will even start “vicariously spying” on victims by spoofing the victim’s number and contacting their friends to ferret out facts that could put the victim in further danger. Although some companies offering spoofing and masking services maintain records to discourage abusive behavior, others take steps to ensure that the true caller’s identity is impenetrably concealed and that the recipient can’t block calls. These features can make it impossible to quell abuse or conclusively prove who’s behind it.

Newfound access to once-sophisticated technologies also presents concerns that seem unlikely to be cured by code anytime soon. “Deep fakes” offer horrific new vectors for abuse, as average people can now create audio and video of their victims doing or saying things they never did or said. Meanwhile, stalkerware applications allow abusers to monitor their victims’ devices and intimate details,
including their locations, messages, pictures, and call logs, while other applications even allow abusers to remotely record video and audio.107 The mere existence of these technologies can instill paranoia in a victim. Their code supports obfuscation, letting abusers evade detection and thwart victims’ attempts to seek protection.108 In many cases, it’s contextually clear who’s using them, but irrefutable proof escapes police and prosecutors who rightly need to meet evidentiary burdens before proceeding.109 It’s like an unfinished whodunit where everyone knows the culprit but the detective disappears before the finale.

Technologists can do much more to code empathetically, but ultimately we need “socio-technological interventions” because improving code won’t completely mitigate digital abuse.110 As danah boyd observes, “[d]esign decisions can inform social practices, but they cannot determine them” because “control is not in the hands of any individual actor—designer, user, engineer, or policymaker—but rather the product of the socio-technical ecosystem.”111 We can’t eradicate digital abuse

---

107 Dell et al., supra note 86; see also BAUM ET AL., supra note 34, at 8 (discussing a 2006 Bureau of Justice Statistics study estimating that 25,000 people were stalked annually via GPS). Astonishingly, services like HelloSpy are overtly branded as tools to track intimate partners. Dell et al., supra note 86. For a deep dive into the terrifying world of stalkerware (or “spyware,” as it’s sometimes called), see Citron, Spying, supra note 6. As Citron reveals, these tools enable “breathtaking” privacy invasions and are often installed on a victim’s device without their knowledge or consent and designed to remain hidden. Id. at 1244–46. Although developers tout seemingly benign uses of the technology—like allowing parents to protect their children—a “key selling point of stalking apps is their hidden nature,” and “stalkers and domestic abusers are often their targeted audience.” Id. at 1246–47. In a commendable move, the Federal Trade Commission has begun to take legal action against these developers for their deceptive and invasive products. See Agreement Containing Consent Order, In the Matter of Retina-X Studios, LLC, File No. 1723118, https://www.ftc.gov/system/files/documents/cases/172_3118_-_retina-x_studios_agreement_containing_consent_order.pdf [https://perma.cc/CW5L-58J2].

108 To make matters worse, the law currently contains a possible escape hatch to enable the companies creating this malware to avoid liability as well. Citron, Spying, supra note 6, at 1248–49, 1252, 1274–75 (discussing how technology companies can evade legal liability under 18 U.S.C. § 2512 for wiretapping and eavesdropping by touting an application’s legitimate uses “as cover for its illegitimate ones”).

109 For background on the difficulties created by online anonymity, see supra note 103.


111 boyd, supra note 103, at 31; see also danah boyd, Networked Privacy, Talk at Personal Democracy Forum 2011 (June 6, 2011) (transcript available at https://www.danah.org/papers/talks/2011/PDF2011.html [https://perma.cc/B3KE-BB64]) (noting that teenagers “invade each other’s privacy in deeply disturbing ways” using online technologies but that “privacy is a networked social process more than it is a structural affordance”).
entirely, and fighting it means waging war on many fronts. When code can’t provide solace, we must focus on building norms of empathy.

II. NORMS-BASED RESPONSES TO DIGITAL ABUSE

Changing norms isn’t an exact science. It involves complex and interlocking factors that no single actor controls. But if we wish to build empathetic norms to counteract digital abuse, one thing is certain: we must raise awareness by speaking out against it and educating people about it.112 When people lack personal experience with abuse, empathy can be a tough emotion to master because it requires imagination.113 Storytelling and education can help to bridge the empathy gap, fostering compassionate perspectives and creating supportive networks for victims of digital abuse.

A. Raising Public Awareness

People need to fathom both the prevalence and severity of digital abuse. Robin West captures this urgency better than I ever could:

Cyber-harassment today is, first, relentlessly cast as the victim’s fault, routinely dismissed as the relatively trivial cost of the much-to-be-desired wild-westiness of the unregulated internet, or the unavoidable price of the free speech rights we all enjoy. Meanwhile the victims are dismissed as whiners, or thin-skinned, or overly sensitive, as incapable of manning up to the slings and errors that go with the territory on the internet, as too dull or humorless to take a joke, as too prone to hystericis to recognize harmless or pathetic barbs when they see them, and as incapable of understanding the importance of First Amendment values.114

Those fighting digital abuse on the front lines tell similar stories. “We misunderstand and minimize this abuse,” warns Erica Olsen of the National Network to End Domestic Violence,115 observing that “people think that if there’s not an immediate physical proximity to the victim, there might not be as much danger.”116 The facts disprove this belief. As we’ve seen, digital abuse exacts a terrible toll on

112 See Citron, Hate Crimes, supra note 6, at 242–50; Citron, Cyber Mobs, supra note 5, at 1091–93.
113 Franks, How to Feel Like a Woman, supra note 11, at 593–94.
116 Id.
its targets. Yet many of the general public fail to grasp how widespread and serious it is.

Raising awareness about digital abuse can generate empathy that directly helps victims. As an initial matter, many people feel unsure if they’re actually victims or not. One striking study revealed that 28% of people who described facing “severe” abusive behavior online (stalking, sexual harassment, sustained harassment, or physical threats) still didn’t consider their own experience to be “online harassment.” This mismatch will resonate with many victims. It takes some people a long time to realize that they’re being victimized and even longer to feel safe or confident enough to speak openly about it. As Adam Smith observed about empathy long ago, “[w]e sometimes feel for another, a passion of which he himself seems to be altogether incapable; because, when we put ourselves in his case, that passion arises in our breast from the imagination, though it does not in his from the reality.”

When people learn more about the realities of digital abuse, they can help victims who are struggling to fathom their own victimization. To be sure, many people are already supportive when victims come forward. Others, however, can accidentally exacerbate feelings of insecurity and shame because they simply lack awareness about the seriousness of digital abuse. If the limits of our language are the limits of our world, we might say that too many people are illiterate about digital abuse. They might be oblivious to how their words and actions make victims feel, but their reactions can become an additional source of harm during a grueling time. Too often, people chastise victims for putting themselves in vulnerable positions or trivialize their experiences. With greater empathy, these reactions might be less common.

A band of invaluable organizations is working to shift norms surrounding digital abuse. The Cyber Civil Rights Initiative, for example, helps victims tackle appalling privacy violations, and a Cornell-based research group is studying how technology is used to perpetrate intimate-partner violence. EndTAB teaches self-
help skills by training people on technical responses to digital abuse,¹²⁵ and organizations like the Anti-Defamation League lobby lawmakers to support victims of online harassment.¹²⁶ Scholars and advocates have also shed light on victims’ experiences by airing abuse stories to the public.¹²⁷ These efforts raise awareness and provide empathetic networks for victims.

To supplement these organizational efforts, there’s an underutilized way to foster empathy for digital-abuse victims: personal narrative.¹²⁸ If victims share their own stories, they can “dispel the myths” about abuse.¹²⁹ Storytelling, especially when imbued with personal narrative, can be a fount of empathy because it offers a potent and accessible way to enhance our imaginations.¹³⁰ Learning about other


¹²⁷ See, e.g., Franks, Unwilling Avatars, supra note 103, at 238–45 (recounting the experiences of various women who suffered digital abuse); Southworth & Tucker, supra note 100, at 668–76; Southworth et al., supra note 95, at 844–50 (presenting empirical evidence—“Stories from Survivors”—of various means of “stalking with technology”); see also Andrew Koppelman, How Citron Changes the Conversation, 95 B.U. L. REV. ANNEX 69, 70 (2015) (praising the norm-changing effects of telling stories about “friends, neighbors, and employers who don’t take [digital abuse] seriously or even blame the victims for allowing it to happen”).

¹²⁸ A similar and powerful methodological tool is autoethnography, but this Essay limits itself to discussing the more accessible tool of personal narrative. See generally CAROLYN ELLIS, THE ETHNOGRAPHIC I: A METHODOLOGICAL NOVEL ABOUT AUTOETHNOGRAPHY xix (2004) (defining autoethnography as “research, writing, story, and method that connect the autobiographical and personal to the cultural, social, and political”).

¹²⁹ See CITRON, HATE CRIMES, supra note 6, at 100.

¹³⁰ Although personal narratives aren’t “traditional fare for the writings and teachings of law professors,” I believe that “the narrative voice is an important, and perhaps underutilized, tool” in legal scholarship. See David W. Case, The Pedagogical Don Quixote de la Mississippi, 33 U. MEM. L. REV. 529, 530 n.2 (2003); see also Mark R. Brown, Affirmative Inaction: Stories from a Small Southern School, 75 TEMP. L. REV. 201, 204–29 (2002) (discussing benefits of narrative in legal scholarship when using personal experiences to discuss affirmative action). One of my favorite examples of using personal narrative in legal scholarship comes from transgender attorney and activist Dean Spade. He used old excerpts from his earlier writings from when he was seeking sex-reassignment surgery as a way to highlight his concerns about relying on medical evaluation of gender identity in legal work toward trans equality. See Dean Spade, Resisting Medicine, Re/modeling Gender, 18 BERKELEY WOMEN’S L.J. 15, 18–23 (2003). He italicized these excerpts while weaving them into his contemporary arguments, thereby allowing his readers to understand how his past experiences informed his present perspectives. Another powerful example comes from my friend Dwayne Betts, who incorporated personal narrative about his time in solitary
people’s suffering through their stories can help us to comprehend the many faces of victimization and harm. Stories, then, can provide a “bridge” to empathetic moral reasoning. 131

Scholars like Martha Nussbaum have explored how literary storytelling can foster imagination and empathy. 132 Nussbaum celebrates “literary imagination” as “an essential ingredient of an ethical stance that asks us to concern ourselves with the good of other people whose lives are distant from our own.” 133 As one review of Nussbaum’s work summarized, she believes that “[e]mpathy is something we practice, and literature helps us to flex this muscle.” 134 Because novels recount the lives of other people, Nussbaum argues, they invite us not only to imagine their experiences, thoughts, and emotions, but also to care about them. 135 Readers begin

131 NUSSBAUM, POETIC JUSTICE, supra note 16, at 12; see also David Bromwich, Rat Poison, 18 LONDON REV. BOOKS (Oct. 17, 1996) (reviewing NUSSBAUM, POETIC JUSTICE, supra note 16), https://www.lrb.co.uk/the-paper/v18/n20/david-bromwich/rat-poison [permalink unavailable] (discussing Nussbaum’s view that novels like Charles Dickens’s Hard Times can reveal “human data” to our imaginations that can build empathy).

132 Nussbaum’s work in this area explicitly draws on Adam Smith, whose discussion of empathy is influential to this Essay’s thesis. See NUSSBAUM, POETIC JUSTICE, supra note 16, at xvi; NUSSBAUM, FROM DISGUST TO HUMANITY, supra note 16, at xviii & n.6; see also Bromwich, supra note 131 (discussing Smith’s influence on Nussbaum’s vision of empathy and imagination). Nussbaum also draws from Roman philosopher and statesman Cicero, whose use of the Latin term humanitas captured “a kind of responsiveness to others that prominently included the ability to imagine their experiences.” NUSSBAUM, FROM DISGUST TO HUMANITY, supra note 16, at xviii n.6.


134 McRobie, supra note 133.

135 See, e.g., NUSSBAUM, POETIC JUSTICE, supra note 16, at 31 (arguing that the novel “gets its readers involved with the characters, caring about their projects, their hopes and fears, participating in their attempts to unravel the mysteries and perplexities of their lives”); Martha C. Nussbaum, The Literary Imagination in Public Life, 22 NEW LITERARY HIST. 877,
to see that “the story is in certain ways their own story” even when its characters appear quite different to them at first blush. This process of “empathic identification” through storytelling can be especially useful in fostering empathy for people who are marginalized and oppressed.

But it’s not only the written novel, or even literature generally, that can provide a window into the lives of others. Stories come in many forms, some more likely to beget empathy than others. An especially effective device is first-person narrative. As Olga Tokarczuk observes, the “authorial self” has a peculiar power to evoke empathetic responses because narrators telling their own stories aren’t mythical “heroes or deities” but rather people who appear “just like us.” First-person narrative can thus connect the narrator and reader through “emotional understanding based on empathy” by blurring the “borders between the narrator’s self and the reader’s self.” This interaction, Tokarczuk claims, creates “a field for the exchange of experiences” that’s conducive to sustaining empathy.

While the fictional novel might expand our imaginative potential, first-person narration of true stories can reveal the actual lived experiences of other people.

---

137 Nussbaum, The Literary Imagination, supra note 135, at 894; see also Nussbaum, Poetic Justice, supra note 16; Aviv, supra note 133 (discussing Nussbaum’s claim that, especially for marginalized or vulnerable groups, justice requires us to “cultivate certain emotions and teach people to enter empathetically into others’ lives”); Bromwich, supra note 131 (discussing Nussbaum’s view that empathy is a “necessary condition for equitable treatment in courts of law” and that judges should look to literature because they “are short of imaginative data about the persons they must judge”). Nussbaum’s later work built on these foundations to outline her vision of the “politics of humanity,” which is a “political attitude that combines respect with curiosity and imaginative attunement.” Nussbaum, From Disgust to Humanity, supra note 16, at xviii. She urges us to build “the capacity for generous and flexible engagement with the suffersings and hopes of other people.” Id. In discussing discrimination, she lauds empathy’s role in advancing and sustaining equality, arguing that “the capacity for imaginative and emotional participation in the lives of others is an essential ingredient of any respect worthy the name.” Id. at xix.

139 Id. at 4.
140 Id.
141 Id. at 5. Despite Tokarczuk’s praise of first-person narration, she cautions against a type of personal narrative that frames the story as “the only one of its kind,” thereby “building an opposition between the self and the world.” Id. at 4. Instead, storytellers must learn from the parable, whose protagonist is more than the “concrete particulars” of their own background. Id. at 5–6. A more empathetic story will entice the reader to look beyond their distinctness and find commonality with people who have experienced “very different fates.” Id. at 6.
Other scholars of digital abuse have already adopted and promoted the use of personal narrative, as did earlier feminist scholars. Telling victims’ stories can be a powerful way to shed light on abuse and influence policy. As Kathryn Abrams observes, “describing events or activities ‘from the inside’—that is, from the perspective of a person going through them—conveys a unique vividness of detail that can be instructive to decisionmakers.” The intensity of reading or hearing victims’ stories can prompt people to take notice of suffering, breaking a cycle of ambivalence and helping victims understand that the abuse isn’t their fault.

Divulging such personal perspectives won’t appeal to everyone, and victims should feel no pressure to tell their tales. It can certainly carry risks, as I know too well. I am, myself, a victim of digital abuse. I had hoped to include snippets of my own story in this Essay, but I ended up omitting all of my personal narrative after several people told me that including it would be too dangerous. Some feared for my physical safety, anxious that telling my story would provoke someone to harm me. Others thought that the professional costs would be too high, especially at this early stage of my career. They worried that sharing details about my experience would lead me to be misjudged by colleagues, overlooked for professional opportunities,

142 See, e.g., Brittan Heller, Of Legal Rights and Moral Wrongs: A Case Study of Internet Defamation, 19 Yale J. L. & Feminism 279 (2007) (using the author’s own victimization as a basis to discuss defamation by anonymous abusers on the internet); Vickery, supra note 56, at 31–45 (relying on the author’s “personal story” because of her belief that we should “share our own stories of disempowerment, intimidation, and harassment as a way to collectively connect our individual experiences to systems of power and oppression”); Waldman, Book Review, supra note 53, at 1947 (discussing how the author’s experiences as an openly gay man, bullied as an adolescent with words like ‘fag’ or ‘queer,’” informs his scholarship on queer online spaces); see also JAMES LASDUN, GIVE ME EVERYTHING YOU HAVE: ON BEING STALKED (2013) (revealing a novelist’s own experience of being cyberstalked by his former student).

143 See, e.g., Susan Estrich, Rape, 95 Yale L.J. 1087, 1087–90 (1986) (recounting the author’s own rape as a prelude to her discussion of “rape law as an illustration of sexism in the criminal law”); see also Kathryn Abrams, Hearing the Call of Stories, 79 Cal. L. Rev. 971, 975 (1991) (discussing the powerful role of first-person narratives in feminist legal scholarship that “bring to light bodily experiences—from the sensations of childbirth to rape to spousal battery—that are not frequently discussed in public, let alone in the pages of law reviews”).

144 Abrams, supra note 143, at 982.

145 See Koppelman, supra note 127, at 70–71 (“Given the anonymity of this [abusive] speech, the best we can hope for may be that the world be more aware of it.”); West, supra note 114, at 80 (suggesting that one reason why law has been slow to respond to digital abuse is that harms are often experienced in private and so go unnoticed).

146 See Franks, Sexual Harassment, supra note 31, at 702 (noting how publicly sharing stories of sexual harassment can “chang[e] the way victims perceive themselves and the problem of harassment, which is in itself a way of changing social norms about acceptable behavior”). At the very least, victims should be empowered to engage in the cathartic exercise of writing and speaking about their experiences even if they choose not to publish anything.
and even denied tenure.\textsuperscript{147} Although many praised my impulse to draw on personal experience in my scholarship, enough people warned me against it that I felt compelled to exclude all details of my own abuse from this Essay.

I believe that the advice I received came from a place of empathy—that people genuinely had my best interests at heart and were trying to protect me from the cruel or callous acts of others. The truth is that they had good reason to worry. When abusers are confronted about their actions, they often deny all allegations and even mount an offensive against their victims.\textsuperscript{148} This retaliation can come in many forms, from untruthfully contradicting the accusations\textsuperscript{149} to spreading lies about the victim\textsuperscript{150} to threatening frivolous legal claims in order to re-exert control and prolong the abuse.\textsuperscript{151} All of these indignities can inflict serious psychological harms on

\textsuperscript{147} I’ll note that not a single person where I work at the University of Georgia raised these professional concerns, making me even more grateful to be joining what seems to be a supportive and empathetic community. Others might not be so lucky. See J. Houl Verkerke, Notice Liability in Employment Discrimination Law, 81 VA. L. REV. 273, 345–46 (1995) (noting that many victims of harassment “fear that a complaint will lead to retaliation” in the workplace).


\textsuperscript{149} See, e.g., James Lasdun, On Being Stalked: A Postscript, JAMES LASDUN, https://jameslasdun.com/give-me-everything-you-have-a-postscript [https://perma.cc/ALS5-RU44] (last visited May 16, 2020) (discussing Lasdun’s experience as a victim of stalking and including an excerpt from the perpetrator’s own memoir where she states that she “stalked no one and made no such threat”); AFARIN MAJIDI, WRITING AND MADNESS IN A TIME OF TERROR: A MEMOIR 3–7 (2017) (responding to Lasdun’s claims of stalking, the perpetrator wrote a remorseful memoir about the experience, explaining her history with mental illness and admitting that she had sent him thousands of emails).

\textsuperscript{150} See, e.g., Southworth & Tucker, supra note 100, at 670 (discussing how abusers “encourage others to contact, harass, or harm the victim,” including by coaxing “others to stalk their victim by posting erroneous and harassing information on websites”). Bobby Chesney and Danielle Citron have voiced concern about the “liar’s dividend,” whereby people use technological tools to deteriorate our sense of truth and enable political manipulation and authoritarianism. See Chesney & Citron, supra note 106, at 1785–86. As they see it, the combination of “truth decay and trust decay” allows bad actors to deny their misdeeds and blame mysterious, unknown actors. Id. at 1786. The liar’s dividend is alive and well in the context of digital abuse, too. Not only do abusers use technology to skirt the law, but they now have the tools to deceive law enforcement and “inhibit a victim’s reality testing.” Southworth et al., supra note 95, at 843; see also infra note 152.

victims, especially when sharing your story leads your abuser—and even authority figures and supposed allies—to engage in “gaslighting” that causes you to doubt your own reality. As Deborah Epstein and Lisa Goodman have shown, victims who are discredited and invalidated after disclosing their abuse commonly develop feelings of powerlessness, futility, personal worthlessness, and self-doubt. Faced with this risk, it’s unsurprising that many victims will retreat and keep quiet.

And herein lies a catch-22. Victims’ stories can help to raise awareness and build empathy, but victims often remain silent because a lack of awareness about digital abuse causes people to lack empathy. Even when victims do speak out, they’ll often be circumspect in what they say for fear of exposing private information, being judged harshly, or antagonizing their abuser. These barriers to storytelling represent an undeniable challenge to my proposal, but not one that’s fatal. We now live in a time when many victims justifiably feel too insecure to share their stories, and so we might lack the foundation for a fully empathetic reaction. But as more victims come forward, the balance will shift—as it already has begun to do.

It pains me to advise victims to share their stories and yet feel incapable of doing so myself. What does it say if even someone in my position of relative privilege—a cisgender, white man and law professor—is urged to stay silent? Yet despite my own experience, I remain convinced that there’s tremendous value in autobiographical storytelling about digital abuse. Though I can’t bring myself to do it, I believe that sharing personal narratives can raise awareness and build empathy. I hope that, in time, more victims will be empowered, not discouraged, to talk about their experiences.

B. Confronting Gender Stereotypes

For too long, the people more commonly targeted by digital abuse have shouldered the burden of addressing it. This pressure adds insult to their injury: they must both face and fight abuse while those who feel disconnected from it stand idly by. We must bring more people into the tent to create empathetic support networks. This means confronting the gender stereotypes underlying society’s views about digital abuse.


152 See Deborah Epstein & Lisa A. Goodman, Discounting Women: Doubting Domestic Violence Survivors’ Credibility and Dismissing Their Experiences, 167 U. PA. L. REV. 399, 447–51 (2019). Digital tools can also contribute to the problem of legal impunity for digital abuse. The same tools that abusers use to stalk and harass their victims can help abusers create doubt about a victims’ claims, engage in “gaslighting,” and even fabricate evidence to make the victim appear to be the perpetrator. When done effectively, this can create enough confusion and doubt in the minds of victims or law enforcement that they’ll simply give up trying to fight or investigate the abuse.

153 Id. at 449–51.
Overwhelming evidence suggests that women face the lion’s share of digital abuse.\textsuperscript{154} Women also experience gender-based abuse at higher rates than men. Among younger men and women, for example, 21% of women report being “sexually harassed” online, over double the share among men.\textsuperscript{155} In addition, many technologies are exploited to inflict grave dignitary harms that tend to harm women disproportionately.\textsuperscript{156}

This gendered reality needn’t create barriers to empathy. Instead, we can enhance empathy across the board by breaking down the gender stereotypes that exacerbate the problem of digital abuse.\textsuperscript{157} A key pathway to doing this is sharing victims’ stories, especially those stories that challenge conventional assumptions underlying these gender stereotypes. Male victims, in particular, should be encouraged to speak out—not to detract from the many female victims of digital abuse, but to stand in solidarity with them and others. In so doing, they can convey how digital abuse features diverse victims and abusers; support the voices of marginalized people who more commonly speak out;\textsuperscript{158} and challenge the gender


\textsuperscript{155} Pew Study 2017, supra note 23, at 7; see also Heller, supra note 142, at 282–83 (discussing, based partly on personal experience as a digital-abuse victim, how women are especially “likely to be hypersexualized,” threatened, and harassed online).

\textsuperscript{156} Thomas E. Kadri, Drawing Trump Naked: Curbing the Right of Publicity to Protect Public Discourse, 78 MD. L. REV. 899, 950–51 (2019) (discussing how women are more often featured in sexualized deep fakes, nonconsensual pornography, and virtual-reality pornography).

\textsuperscript{157} See Ali Miller, Fighting Over the Figure of Gender, 31 PACE L. Rev. 837, 871 (2011) (“Just as we must assure ourselves that we all benefit from justice across race, ethnicity, religion, age, and nation, I suspect fundamentally we may also have to reassure ourselves that we all benefit from liberation from gender binaries and sexual repressions.”).

\textsuperscript{158} Many of the prominent legal scholars who write about digital abuse are women (e.g., Danielle Citron, Mary Anne Franks, and Karen Levy) and gay men (e.g., Ari Waldman). In my experience, it’s rare for men—especially cisgender, white men—to speak out about these issues.
essentialism that impedes true empathy. As one empirical study concluded, “unless we uproot the simplistic stereotypes that limit understandings about sexual victimization, we will not address it accurately, nor will we respond to victims empathically.”

In practical terms, how can we confront gender stereotypes? As an initial matter, education and awareness efforts should recognize that the bulk of digital abuse targets women without making men feel that being abused is humiliating or aberrant. Too often, men face an expectation that they must avoid situations that counter their stereotypical roles as men. This societal pressure can translate into a reluctance to identify as an abuse victim. Empirical evidence shows that men fear disclosing sexual assault and seeking help. Instead, they resort to “heteronormative scripts appropriated to make sense of sexual victimization”—scripts suggesting that “victimhood is largely incompatible with dominant notions of masculinity.” The ripple effects are significant. Male victims suffer from feelings of shame and embarrassment, blame themselves, and fret that they won’t be believed if they speak up. These “masks of masculinity” reduce disclosure of abuse and contribute to serious underreporting by male victims. They also inhibit

---


160 See Angela P. Harris, Heteropatriarchy Kills: Challenging Gender Violence in a Prison Nation, 37 WASH. U. J.L. & POL’Y 13, 16–17 (2011) (describing how “toxic” and “destructive” masculinity depends on men “not being a woman, and not being gay,” and often relies on violence as a way of reclaiming it). See generally Angela P. Harris, Gender, Violence, Race, and Criminal Justice, 52 STAN. L. REV. 777 (2000) (exploring the connection between masculinity, race, and violence in the criminal justice system).

161 Heather R. Hlavka, Speaking of Stigma and the Silence of Shame: Young Men and Sexual Victimization, 20 MEN & MASCULINITIES 482, 482 (2017); Lara Stemple & Ilan H. Meyer, The Sexual Victimization of Men in America: New Data Challenge Old Assumptions, 104 AM. J. PUB. HEALTH 19, 21 (2014) (“Feelings of embarrassment, the victim’s fear that he will not be believed, and the belief that reporting itself is unmasculine have all been cited as reasons for male resistance to reporting sexual victimization.”).

162 Hlavka, supra note 161, at 482.

163 Id. at 482–83, 499–500.

164 Id. at 482; see also Stemple et al., supra note 159, at 303 (asserting that “persistent minimizing of male victimization” can rest on both “gender stereotypes” and “outdated definitions of sexual victimization”); id. at 308–09 (noting that victims of female-initiated abuse face disclosure obstacles that obstruct their ability to “access healthcare, recovery support, and legal redress”).
understanding of the phenomenon of male victimization, chilling research in an area that’s already underappreciated and understudied.\(^{165}\)

Despite the efforts of many existing support networks to use gender-inclusive language,\(^{166}\) “[t]he dominant script for boys and men is to be brave, stoic, and to deal with problems alone.”\(^{167}\) This narrative can inflict at least two distinct injuries. Stereotypes about masculinity can keep men in dangerous positions for longer by making them reluctant to admit their abuse and take steps to end it. And those same stereotypes can keep men in harm’s way even after they report abuse as they face skepticism about their victimization from male-dominated institutions like law enforcement and the judiciary.\(^{168}\) The situation is likely worse when men are victims of female-perpetrated abuse, as studies reveal that female abusers “are less likely to be investigated, arrested, or punished compared to male perpetrators, who are regarded as more harmful.”\(^{169}\) These studies, in turn, fit within a larger tale of “precarious manhood,” in which masculinity is “seen as a precarious state requiring continual social proof and validation.”\(^{170}\) This precariousness leads men to feel especially threatened by challenges to their masculinity.\(^{171}\) Since victimization and


\(^{167}\) Hlavka, \textit{supra} note 161, at 486.


\(^{169}\) Friedersdorf, \textit{supra} note 165; see also Stemple et al., \textit{supra} note 159, at 309 (discussing how “female perpetration is downplayed by those in fields such as mental health, social work, public health, and law”).


Masculinity are often perceived as incompatible, men who admit abuse frequently endure suspicion and even hostility.

Embracing the reality of male victimization is consistent with feminist efforts to combat gender-based abuse. For one thing, recognizing male victimization challenges restrictive and harmful constructions of masculinity that contribute to abuse across gender and sexuality spectrums. Not only are men harmed by the misimpression that they’re immune from abuse (as various studies of “rape myths” have shown), but women also suffer from “the hegemonic notions of masculinity that underpin misogyny” and that perpetuate “regressive gender norms.” Heterosexist assumptions about abuse also hurt LGBTQ and nonbinary people by delegitimizing the dynamics of their victimization. And destructive notions of masculinity can encourage men “to disconnect from their emotions, objectify and degrade women, debase homosexuality, and resolve conflicts through violence.” Nobody wins; everybody loses.

Facing up to male victimization also challenges pernicious gender essentialism, which denies autonomy to both men and women. By claiming that men and women have roles assigned to them at birth, gender essentialism “forbids men and women from taking up contrary roles.” In a related context, Mary Anne Franks confronts gender essentialism by considering how men who are sexually assaulted

---


173 Stemple et al., supra note 159, at 304 (discussing surveys showing that majorities of college students don’t believe that a “big, strong man can be raped by a woman” or that a man who’s raped by a woman would be “very upset”); see also Michelle Davies & Paul Rogers, Perceptions of Male Victims in Depicted Sexual Assaults: A Review of the Literature, 11 AGGRESSION & VIOLENT BEHAV. 367 (2006) (detailing how male victims are viewed as more culpable for experiencing sexual abuse if their abuser is female rather than male).

174 Vickery, supra note 56, at 45.

175 Stemple & Meyer, supra note 161, at 20.

176 See Brown et al., supra note 81, at 211 (noting “the need to create more fluid understandings of gender so as not to exclude violence among couples in the LGBT community, or minimize the perpetration of violence toward males” (citing Gwen Hunnicutt, Varieties of Patriarchy and Violence Against Women: Resurrecting “Patriarchy” as a Theoretical Tool, 15 VIOLENCE AGAINST WOMEN 553 (2009))); Stemple et al., supra note 159, at 303, 308–09 (reporting that “[l]esbian and bisexual women abused by women report feeling that their victimization is delegitimized due to heterosexist assumptions” and “frequently hesitate to report due to fear of heterosexist social attitudes”); id. at 309 (arguing that “stereotypical understandings of women as sexually harmless” are problematic because “[h]eterosexism can render lesbian and bisexual victims of female-perpetrated sexual victimization invisible to professionals”).

177 Hlavka, supra note 161, at 499–500.

178 Franks, How to Feel Like a Woman, supra note 11, at 574.

179 Id.
in prison describe being “treated like a woman.” As Franks notes, “feminization is punitive for both men and women” when it’s used as a proxy for subordination. We make no progress if men facing abuse are seen as victims only because they’re being treated “like a woman”—that is “degraded, dehumanized, and sexualized.”

Franks rightly asserts that “[t]he proper approach to assessing forced feminization is to focus on its oppressive structure, not on the gender of its victims.” I share her hope that, when we do so, “we can see what all victims along the spectrum of sexual and domestic abuse have in common, and we can form social and legal responses accordingly.” If we fail to recognize the complex interactions between gender and digital abuse by viewing abuse as a “women-only” issue, we might inadvertently naturalize female subordination and delegitimize male victimization. Such a failure robs us of empathetic resources. We shouldn’t tempt men who aren’t victimized to distance themselves from abuse so easily.

By missing the thicker story about gender and digital abuse, we also contribute to a vision of harassment that paints women as vulnerable and “one-dimensional.” Education efforts that focus purely on threats to women play into stereotypes about female weakness and risk associating sex purely with danger. Worse still, they

---

180 Id. at 568–72.
181 Id. at 568.
182 Id.
183 Id.
184 Id.
185 Stemple et al., supra note 159, at 304; see also Gayle S. Rubin, Thinking Sex: Notes for a Radical Theory of the Politics of Sexuality, in CULTURE, SOCIETY AND SEXUALITY: A READER 143, 166 (Richard Parker & Peter Aggleton eds., 1999); Miller, supra note 157, at 841 & n.4 (discussing how some conceptions of “gender-based violence” that effectively exclude heteronormative men can harm both men and women); Stemple & Meyer, supra note 161, at 20 (noting that “contemporary gender theorists have questioned the overwhelming focus on female victimization, not simply because it misses male victims but also because it serves to reinforce regressive notions of female vulnerability” that “can perpetuate norms that see women as disempowered victims”). See generally MYRIAM S. DENOV, PERSPECTIVES ON FEMALE SEX OFFENDING: A CULTURE OF DENIAL (2004) (discussing traditional societal sex roles in which women are construed as nurturing, protecting, nonaggressive, and nonsexual); JANET HALLEY, SPLIT DECISIONS: HOW AND WHY TO TAKE A BREAK FROM FEMINISM 346 (2006) (“While feminism is committed to affirming and identifying itself with female injury, it may thereby, unintentionally, intensify it.”).

186 See Katherine M. Franke, Theorizing Yes: An Essay on Feminism, Law, and Desire, 101 COLUM. L. REV. 181, 199–202 (2001) (suggesting that we might “want to de-sacrilize the sex-danger alchemy within feminist legal theory—not to ignore the significance of sexual violence for women, but instead to de-essentialize sex’s a priori status as a site of danger for women and one best cleansed of such danger”); Arlene Stein & Andrea Press, Pleasure & Danger: Exploring Female Sexuality, 30 BERKELEY J. SOC. 205, 205 (1985) (observing that many feminists argue that the attention paid to “sexual danger . . . has led to the marginalization of notions of female pleasure”); Carole S. Vance, More Danger; More Pleasure: A Decade After the Barnard Sexuality Conference, 38 N.Y.L. SCH. L. REV. 289,
feed a victim-blaming culture that expects women to take the lead in preventing their own abuse. The impulse to blame victims need not be malicious, but even well-meaning suggestions out of concern for victims’ safety can provoke feelings of guilt: change your phone number, delete your social media, move to a different place, get a security system, come up with a good “story” to tell potential employers, keep quiet about this, don’t tell the police. There’s a fine line between encouraging victims to engage in self-help and making them feel complicit in their abuse. Education efforts must be sensitive to that distinction.

Consider the Megan’s Story advertising campaign, which warned against the dangers of “sexting” through a video depicting a teenager’s nightmarish experience after sending a nude photo to a classmate. The campaign was styled as a “safety film,” suggesting that the inevitable consequences of sexting are humiliation and shame. But sexting can, in some circumstances, be a valuable form of expression that enriches relationships. The campaign, however, missed all nuance, evoking a “risk management” model of abuse education that defines women as inherently at risk of sexual abuse and responsible for predicting, avoiding, and managing that risk. As one blogger critically noted in response to the campaign, “[i]magine a drink-driving ad that showed a pedestrian being run over, the car zooming away, and then a caption that said ‘Watch where you’re walking, pedestrians.’”

290 (1993) (arguing that a feminist approach to sexual matters should “simultaneously . . . reduce the dangers women face and . . . expand the possibilities, opportunities, and permissions for pleasure that are open to them”).


188 Kath Albury & Kate Crawford, Sexting, Consent and Young People’s Ethics: Beyond Megan’s Story, 26 CONTINUUM: J. MEDIA & CULTURAL STUD. 463, 463–65 (2012).

189 Id. at 463–65.

190 Id. at 464; see also id. at 466–49 (presenting qualitative empirical evidence of young people’s use of sexting, including examples where the practice was “positive” and helped to enhance and maintain relationships). The written materials accompanying the campaign painted a more nuanced picture, encouraging students to discuss gender stereotypes and develop alternate endings to the video depending on the actions of Megan’s classmates. Id. at 465.

191 Id. at 465.

education model, in which abusers are absent and victims are shamed, is deeply flawed.\textsuperscript{193}

We must also do more to alter men’s attitudes about digital abuse. A recent study revealed that 73\% of men aged 18 to 29 feel that “many people take offensive online content too seriously.”\textsuperscript{194} And while 70\% of women think online harassment is a “major problem,” only 54\% of men feel the same way.\textsuperscript{195} These statistics hint at a deeper problem of how many men devalue behavior that disproportionately harms women—a problem that results in a dearth of empathy. “[I]n lieu of genuine empathy, men’s response to the sexual abuse of women generally takes three troubling forms: pathological (neither sympathetic nor empathetic), sympathetic (but not empathetic), and superficially empathetic.”\textsuperscript{196}

To help change these dire realities, men should be more involved in education and awareness efforts surrounding digital abuse. Male victims, in particular, should play an active role. The reasons are twofold—one regrettable, the other less so. The more benign reason to illuminate male victimization is that it grabs people’s attention and signals that abuse is harmful across different gender dynamics. People assume that digital abuse is rare and that abuse of men is rarer still. By featuring male victims in awareness efforts, we can disrupt false assumptions in memorable ways and erode detrimental stereotypes.

The second, more unfortunate, reason to feature men in these efforts is that it might make some male decisionmakers more eager to address victimization across the gender spectrum. As Robin West rhetorically asks when discussing digital abuse: “So, where are the police, the prosecutors, the courts, the judges and the lawyers?”\textsuperscript{197} The sad reality, I fear, is that many of them are men who don’t feel invested in this issue. They maintain a safe distance from those suffering from digital abuse, at most expressing pity when they hear tales of female victimization. Put simply, they lack empathy. Revealing the realities of male victimhood could foster change at the margins.\textsuperscript{198}

Those involved in efforts to shift norms surrounding digital abuse can learn lessons from other movements for social change. It would certainly be nice if telling stories about other people’s suffering was enough to trigger empathy. But when that

\textsuperscript{193} See Wildly Parenthetical, supra note 192 (explaining how the Megan’s Story campaign perpetuates “a way of thinking that says that girls and young women are perpetually at risk, and that those risks are their responsibility”).

\textsuperscript{194} PEW STUDY 2017, supra note 23, at 8.

\textsuperscript{195} Id.

\textsuperscript{196} Franks, How to Feel Like a Woman, supra note 11, at 598–600.

\textsuperscript{197} West, supra note 114, at 80.

\textsuperscript{198} See Franks, How to Feel Like a Woman, supra note 11, at 604 (making similar arguments about enlightening people to the abuses suffered by men in prison as a way “to reduce the social tolerance of sexual abuse more generally”).
suffering is tied to power differentials, the realpolitik counsels us to tell stories in a particular kind of way—to highlight aspects of stories that seem likely to elicit empathetic responses from privileged groups. Especially when storytelling seeks to stimulate empathy for marginalized people, there’s value in stressing points of commonality that reveal similarities in interests. As Derrick Bell has taught us in the context of racial justice, a movement for social change usually has a greater chance of success if it can persuade privileged groups that their welfare is connected to the fates of those who are traditionally marginalized.199

Applying Bell’s idea of interest convergence to the movement against digital abuse, privileged and powerful actors might be more likely to develop empathy for victims if they believe their interests are similar.200 Revealing truths about male victimization could be an important part of this strategy. These efforts shouldn’t erase the important differences between people, for that would contradict the empathetic goal of replacing self-interest with fellow-feeling. Indeed, it’s crucial to unpack how various social markers of difference—gender, race, sexual orientation, and so on—play into people’s suffering.201 But an intersectional approach to suffering isn’t antithetical to an empathetic approach. We can all benefit from understanding the full scope and shape of abuse, and empathy can help us to do that.

It’s worth stressing again that confronting gender stereotypes surrounding digital abuse shouldn’t come at women’s expense, nor should it detract from paying essential attention to male-perpetrated abuse.202 We should also be wary of what Mary Anne Franks calls “injury inequality,” whereby social or legal systems

\[\text{\textsuperscript{199} I thank Danielle Citron for drawing my attention to the similarities between my views on empathy and Bell’s work on interest convergence in the context of racial justice. See Citron, Cyber Civil Rights, supra note 59, at 84 (discussing how Bell’s work “counsel[s] that civil rights progress is most likely to occur when the interests of vulnerable people can be aligned with those of the dominant group”); see also Derrick Bell, And We Are Not Saved: The Elusive Quest for Racial Justice 63–74 (1987) (explaining how progress for racial justice generally depends on convincing white people that they will also benefit); Derrick A. Bell, Jr., Comment, Brown v. Board of Education and the Interest Convergence Dilemma, 93 Harv. L. Rev. 518, 523 (1980); cf. Richard Delgado & Jean Stefancic, Critical Race Theory: The Cutting Edge xvi–xvii (2d ed. 2000) (arguing that “white elites will tolerate or encourage racial advances for blacks only when such advances also promote white self-interest”).}

\[\text{\textsuperscript{200} See also Smith, supra note 10, at 9 (“His agonies, when they are thus brought home to ourselves, when we have thus adopted and made them our own, begin at last to affect us, and we then tremble and shudder at the thought of what he feels.”)).}

\[\text{\textsuperscript{201} See generally Kimberle Crenshaw, Mapping the Margins: Intersectionality, Identity Politics, and Violence Against Women of Color, 43 Stan. L. Rev. 1241, 1242 (1991) (discussing how an intersectional approach shouldn’t conflate or ignore intragroup differences).}

\[\text{\textsuperscript{202} See Stemple et al., supra note 159, at 303–04.} \]
exaggerate injuries affecting the privileged while downplaying those affecting the marginalized.\textsuperscript{203} As Franks observes, injury inequality leads to practical pathologies:

\begin{quote}
[It] preserves the lion’s share of resources for addressing the injuries of the privileged, leaving little for those already less equipped to cope with injury. While elites can expect that their injuries will be accommodated in the structure of law and society itself, the marginalized must make do with self-help. The effect is not limited to economic, legal, or physical resources, but extends to psychological resources. Injury inequality discourages empathy and compassion to the harms suffered by the less powerful.\textsuperscript{204}
\end{quote}

Kate Manne has memorably dubbed this phenomenon “himpathy” when it features the all-too-common “flow of sympathy away from female victims toward their male victimizers.”\textsuperscript{205} Manne worries that “empathy can make us take sides with the historically dominant, against the less privileged,” and “that lionizing empathy can ask for and extract too much from women.”\textsuperscript{206} It bears noting, too, that some injuries caused by digital abuse might be felt more acutely when victims are already marginalized institutionally, as is often the case for women and sexual minorities.\textsuperscript{207}

Given existing inequalities in our society, it’s understandable to worry that highlighting male victimization might detract from efforts to help those likelier to suffer from digital abuse.\textsuperscript{208} While I appreciate this concern, I’m convinced that presenting a fuller picture of digital abuse will bring benefits across the board. Nothing proposed in this Essay should countenance injury inequality, which relies on exaggerating privileged injury or downplaying marginalized injury (or, worse still, doing both simultaneously). For example, a system would exhibit injury

\textsuperscript{203} Franks, Injury Inequality, supra note 154, at 231; cf. Alice E. Marwick & Robyn Caplan, Drinking Male Tears: Language, the Manosphere, and Networked Harassment, 18 FEMINIST MEDIA STUD. 1, 3–5, 11 (2018) (discussing the historical lineage between the 1970s “Men’s Rights Movement”—which “acknowledged that sexism harmed women, but emphasized that strict gender roles and patriarchal society were equally harmful to men”—and the present-day “manosphere”—which includes “diverse communities brought together by a common language that orients them in opposition to the discourse and rhetoric of feminism”).

\textsuperscript{204} Franks, Injury Inequality, supra note 154, at 231.


\textsuperscript{206} Id. at 200 n.14.


\textsuperscript{208} See supra notes 154–156.
inequality if it inflated the harm that men face when they’re accused of sexual assault while minimizing the harm done to women who are assaulted. Injury inequality, then, rests on belittling harm to marginalized people or aggrandizing harm to privileged people.

That is emphatically not my project. Instead, I seek to show that people who enjoy privilege in many aspects of their lives can suffer serious injury due to digital abuse—and that there are widespread benefits to raising awareness of that fact. Indeed, there are ways that a victim’s own privilege can even exacerbate abuse in some circumstances. Yet many men mistakenly view anti-abuse efforts “as a zero-sum game: if women gain, then they lose.” This must change. Each of us has a responsibility to address abuse and the structural forces that sustain it. We should promote diverse voices in these efforts, recognizing, as Carol Hanisch did years ago, that “[t]here are no personal solutions at this time,” but “only collective action for a collective solution.”

C. Building Institutional Support

Normative reforms can stem from institutions. Institutional actors can, at their best, shape empathetic norms and then prevent backlash and backsliding. They can also provide crucial support networks for digital-abuse victims when empathy is needed most. Just as the general public needs to understand the realities of digital abuse, so too must institutional actors who often encounter abusers and victims. Effective institutional support requires procedures and training animated by empathy.

Many institutional actors would benefit from greater empathy for digital-abuse victims. I’ve already discussed how technology companies should integrate empathy into their design processes—a move that partly depends on creating empathetic norms within those corporate institutions. But when coding fails to scupper digital

209 Franks, Injury Inequality, supra note 154, at 240–43; cf. infra notes 234–236 and accompanying text (discussing the new Department of Education policies in Title IX cases).

210 There are some similarities between my arguments and those found in recent work on white privilege by critical race theorist Khiara Bridges. See Khiara M. Bridges, Race, Pregnancy, and the Opioid Epidemic: White Privilege and the Criminalization of Opioid Use During Pregnancy, 133 HARV. L. REV. 770, 771 (2020) (arguing that “white privilege is a double-edged sword” in that it “can lead to unfavorable results just as capably as it can lead to favorable ones”); Khiara M. Bridges, White Privilege and White Disadvantage, 105 VA. L. REV. 449, 482 (2019) (observing that “white privilege is a dangerous thing—both for those who are unprivileged by virtue of it, as well as for those who possess it”). Although I don’t have the space to tease out these similarities in this Essay, I’ll note my belief that scholars of digital abuse can learn a lot from Bridges’s work.

211 Vickery, supra note 56, at 45.


213 See supra Section I.A; Sylvain, supra note 41, at 252.
abuse, which other institutional actors could diminish its attendant harms through social norms? Many people can be effective “norm entrepreneurs,”"214 but this Essay focuses on two groups frequently in the trenches fighting digital abuse: (1) law enforcement professionals and (2) educators and employers.

First, the professionals who investigate, prosecute, judge, and treat digital abuse.215 Influencing these actors’ attitudes is vital because, sometimes, “we lack not laws but law enforcement.”216 To be fair, underenforcement can begin with victims themselves, who often don’t report or reveal abuse. Many victims are simply unaware of the legal ramifications of digital abuse,217 while structural factors impede other victims’ willingness to admit their abuse, such as when the relationship dynamics transgress gender stereotypes.218 Even when victims do disclose abuse, the vast majority won’t confide in the police.219

214 See Cass R. Sunstein, Social Norms and Social Roles, 96 COLUM. L. REV. 903, 909 (1996) (defining “norm entrepreneurs” as “people interested in changing social norms”); see also id. at 929, 947–52 (further explaining how various private and public actors can be effective “norm entrepreneurs”).

215 I lack the expertise to speak about how cultural and structural issues in many police departments might make my proposals unrealistic. I have concerns that some of the extralegal reforms I suggest wouldn’t be embraced by many within law enforcement. See generally Leigh Goodmark, Hands Up at Home: Militarized Masculinity and Police Officers Who Commit Intimate Partner Abuse, 2015 BYU L. REV. 1183, 1183 (exploring intimate partner abuse by police and arguing that “[c]hanging the behavior of abusive police officers may be nearly impossible given the interplay of policing and masculinity”). Despite my skepticism, I offer these proposals aspirationally because it’s so important to promote greater empathy within this particular institution.

216 Jane R. Bambauer & Derek E. Bambauer, Cyber-Exploitation and Distributed Enforcement, 95 B.U. L. REV. ANNEX 37, 37 (2015); see also CITRON, HATE CRIMES, supra note 6, at 83 (asserting that social attitudes can lead to underenforcement of criminal harassment laws).

217 Cf. Albury & Crawford, supra note 188, at 465–66, 469 (observing that many teenagers are aware of the legal penalties they might face for sexting).

218 See supra Section II.B.

219 One study revealed that, of people who responded in some way to digital abuse, only 5% reported it to law enforcement. PEW STUDY 2014, supra note 23, at 6. There’s reason to believe that this hesitancy to report might be greater among male victims. See Stemple & Meyer, supra note 161, at 21 (“Although state laws have become more gender neutral, criminal prosecution for the sexual victimization of men remains rare and has been attributed to a lack of concern for male victims.”). Empirical evidence suggests that when the perpetrator is female, male victims are even less likely to involve law enforcement and, even if they do, are less likely to be taken seriously by an array of institutional actors in the justice system. See Stemple et al., supra note 159, at 309 (discussing how female-on-male abuse is often underreported to police, downplayed by healthcare professionals and law enforcement, and less likely to result in criminal convictions).
When victims do find the courage to involve law enforcement, they’re frequently met with indifference, even if there’s compelling evidence.220 It’s especially unfortunate when officers sever digital abuse from physical abuse and focus only on the latter, for one so often leads to the other as part of an interwoven scheme of escalation and control.221 Victims are too often left to fend for themselves while “officers refuse to do anything because, in their view, the abuse is too personal, too messy, and too difficult to address.”222 As incidents of digital abuse increase and evolve, police departments should work with experts to respond.223 Organizations like EndTAB are providing training programs for officers across the country, as well as for other institutional actors who might collaborate with law enforcement.224 Similar initiatives seek to train victims who might then be in a better position to educate law enforcement about their abuse. A group of technologists from Cornell and New York University, for example, is working with the New York City mayor’s office to train and support victims.225 Other cities should prioritize similar efforts.

Ultimately, it takes money to provide the kind of guidance that could shift norms and avert non-empathetic responses from law enforcement. As Amanda Hess has reported, investigating and prosecuting cases of digital abuse is “still largely a problem of resources, not just know-how.”226 Part of the struggle is convincing state lawmakers and treasurers that digital abuse is worthy of significant resources—a process that could be ignited by the kinds of awareness-raising efforts advanced in this Essay. In the interim, technology companies should facilitate—and even fund—these kinds of training, which should be understood as a part of corporate social responsibility in the industry. Even if neither industry nor government devotes

220 CTRON, HATE CRIMES, supra note 6, at 20–21; see also Bambauer & Bambauer, supra note 216, at 37 (remarking that laws prohibiting online stalking, harassment, and revenge porn “provide little benefit if they lie unused”).

221 See generally Diana Freed et al., “A Stalker’s Paradise”: How Intimate Partner Abusers Exploit Technology, ASS’N COMPUTING MACH. (2018) (presenting qualitative research of how domestic abusers exploit technologies to intimidate, threaten, monitor, impersonate, harass, or otherwise harm their victims); Diana Freed et al., Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders, 46 PROC. ASS’N COMPUTING MACH. HUM.-COMPUT. INTERACTION 1 (2017) (same).

222 CTRON, HATE CRIMES, supra note 6, at 20.

223 See Citron, Spying, supra note 6, at 1249, 1268, 1279 (emphasizing the importance of training police and providing them with forensic equipment necessary to investigate digital abuse).


225 See O’Neill, supra note 110.

additional dollars to this issue, more can be done with what’s already in the kitty. Different localities should form networks to share digital-forensics resources and fund officer training, while lawmakers could support these collaborative efforts by insisting that fines imposed for cyber-harassment go toward funding specialists and education efforts.227

Looking beyond law enforcement, a second group of institutional actors would gain from empathetic consciousness: people in places of education and employment. Digital abuse often affects students and educators, employees and employers, and the administrators and staff who make their institutions function. Scholars like Danielle Citron have already done valuable work on the benefits of educating young people about digital abuse,228 so I make only two ancillary points. First, although many education efforts rightly focus on teenagers, it’s worth noting that 67% of people aged 18 to 29 have experienced some form of digital abuse, as have 49% of people aged 30 to 49 and 22% of people above 50.229 Education efforts mustn’t end “at the schoolhouse gate”—or at least not at the end of high school.230 Adults deserve attention as both victims and abusers, and employers and universities should spearhead education efforts.231 Given that many abusers are adults, we must hope that, on this issue, we can teach older dogs new tricks.

Second, civil rights laws must be sensitive to the dynamics of digital abuse. Although the limited jurisdictional scope of Title VII and Title IX means that these laws won’t cover a lot of online harassment,232 employers and universities can play crucial roles in building empathetic support networks. The need is obvious: one in eight stalking victims reports losing work because of the abuse, and the effects are often far worse than reduced productivity.233

---

227 See Citron, Spying, supra note 6, at 1277.
228 See, e.g., Citron, Hate Crimes, supra note 6, at 242–50; Citron, Cyber Mobs, supra note 5, at 1091–93.
231 See Brown et al., supra note 81, at 210, 212–15 (reviewing limited research on digital abuse among adults and concluding that “there is ample space in the literature for more recent research on online abuse among more diverse populations of adult victim-survivors”); Feldman, supra note 1 (discussing the need for education beyond high school because digital-abuse literacy is crucial for adults and “not just kids”).
233 Baum et al., supra note 34, at 7; see also notes 29–38 and accompanying text.
Despite the need for strong civil rights protections for abuse victims, President Trump’s administration seems more concerned with the rights of the accused than the wellbeing of accusers.\(^{234}\) Thanks to procedural changes to allow in-person cross-examination of students who report sexual misconduct, some schools are considering scrapping formal Title IX hearings altogether for fear that the process will become too traumatic.\(^{235}\) Even if schools maintain the hearings, the new regulations might discourage victims from coming forward.\(^{236}\) These regulatory moves are unwise and should be repealed, and resources should be devoted to training administrators to recognize and respond to digital abuse—and to show empathy for its victims when they see it.

CONCLUSION

Missing from this Essay is much talk about legal responses to digital abuse. My focus, instead, has been on code and norms. But don’t be fooled: law should play a crucial role. After all, as Ryan Calo cautions, some people are “dedicated in their hate; they will ignore norm entrepreneurship and find ways to end run technical controls.”\(^{237}\) Lawmakers should have more empathy for victims,\(^{238}\) and the law should empower and protect victims more than it currently does.\(^{239}\) Moreover, the


\(^{235}\) Id.

\(^{236}\) Id.


\(^{238}\) On the relationship between law and empathy, see, for example, Lynne N. Henderson, Legality and Empathy, 85 Mich. L. Rev. 1574, 1576 (1987) (arguing that empathy “is a rich source of knowledge and approaches to legal problems—which are, ultimately, human problems”), and Toni M. Massaro, Empathy, Legal Storytelling, and the Rule of Law: New Words, Old Wounds?, 87 Mich. L. Rev. 2099, 2123–24 (1989) (discussing the challenges of squaring empathy with legal decision-making but suggesting ways that empathetic reasoning can help legislators and judges).

\(^{239}\) Scholars like Danielle Citron and Mary Anne Franks have urged legislators to adapt both tort law, criminal law, and civil rights law to address digital abuse. See, e.g., Citron, Hate Crimes, supra note 6; Mary Anne Franks, Question: How Can the Law Respond to Online Harassment?, in Mediating Misogyny: Gender, Technology, and Harassment 404, 404–05 (Jacqueline Ryan Vickery & Tracy Everbach eds., 2018); Mary Anne Franks, The Banality of Cyber Discrimination, or, the Eternal Recurrence of September, 87 Denv. L. Rev. Online 5, 8 (2010), https://maryannefranks.com/post/115428385438/the-banality-of-cyber-discrimination-or-the [https://perma.cc/BM5K-ERLX]; Franks, Sexual Harassment, supra note 31, at 696; see also Quick Guide to Stalking: 16 Important Statistics, and What You Can Do About It, NAT’L COAL. AGAINST DOMESTIC VIOLENCE (Jan. 30, 2017), https://ncadv.org/blog/posts/quick-guide-to-stalking-16-important-statistics-and-what-you-
law has “expressive value” that can “change our cultural software” and positively influence code, norms, and markets.

Yet while law can do more, legislation can’t eradicate digital abuse without eviscerating the many benefits of digital technologies. Sophisticated technologies can also evade sophisticated legal interventions, and even unsophisticated digital abuse can be tough to fight “because the relationship between abuser and victim is socially complex.” We must therefore regulate harmful behavior through extralegal forces as well.

I’ve argued that efforts to address digital abuse through code and norms should be animated by empathy for victims. Instead of detaching ourselves from the can-do-about-it (endorsing legislation to fund programs to combat abuse, such as those established by the Violence Against Women Act). States could, for example, allow civil actions for certain types of digital abuse, with the provision of court costs and attorney’s fees if the victim’s claim is successful. They could also mandate forms of recordkeeping by purveyors of technologies that are frequently used to stalk and harass, such as prepaid phones and spyware applications. See Citron, Spying, supra note 6, at 1276–77 (discussing recordkeeping requirements that lawmakers could impose on stalkerware providers). Empathetic legislation might also include protections for pseudonymous litigation, whereby victims could presumptively file under assumed names to protect their privacy. See Daniel J. Solove, The Future of Reputation: Gossip, Rumor, and Privacy on the Internet 190–91 (2007) (contending that the presumption favoring real-name litigation should disappear when the nature of the allegations would prevent victims from asserting their rights); Citron, Hate Crimes, supra note 6, at 162–63 (discussing various proposals for pseudonymous litigation in digital-abuse cases).


See Citron, Hate Crimes, supra note 6, at 128.

Levy, supra note 98. As Levy observes: “What’s difficult about protecting the privacy and security of victims isn’t technical complexity; it’s that the relationship between the abuser and the victim involves social, physical, financial, and emotional ties, and that digital abuse is deeply intertwined with all of these.” Id.
experiences of others, we can create a more comprehensive understanding of harm by engaging our imaginations and attempting to feel as others feel. Storytelling by victims can help to build empathy and persuade privileged actors that their interests align with the more marginalized in society. This blueprint for empathy builds on longstanding and essential work to oppose the trivialization of digital abuse.\textsuperscript{243} Supported by that foundation, we can now be more ambitious. We should engage our imaginations to blur the boundaries between those who’ve suffered abuse and those who haven’t; we should listen to victims’ stories and strive to feel as they feel. By building networks of empathy, we can better address the many harms that digital abuse can bring.

But what’s to stop abusers from weaponizing empathy? If empathetic resources are as powerful as I claim, abusers might deploy the language of victimhood to further their harmful conduct or escape its consequences. There’s no easy fix to this problem, and we often see manipulative role-reversals when victims disclose their abuse.\textsuperscript{244} Yet having empathetic responses to claims of victimization doesn’t mean believing all accusations, nor does it mean ignoring society’s existing power structures. Certain institutional actors, particularly those in law enforcement, have truth-seeking duties that require scrutinizing the veracity of abuse claims. Empathy, however, remains a sound first response—a starting point in seeking to understand alleged abuse and an animating principle going forward. When all is said and done, empathy’s value is worth its potential misuse.

This brings me to a final, slightly painful, point. While my focus has been on victims, we should strive to have empathy for abusers, too. Not only might they sometimes deserve compassion,\textsuperscript{245} but understanding the social complexity of digital abuse also requires an appreciation of why abusers act as they do. My parting call to empathize with abusers might strike some people as unwarranted and even unjust to victims, and I admit I struggle to heed my own advice. I’ve tried to empathize with my abuser, and it’s a constant struggle. Nevertheless, despite the difficulty, we must understand both sides of the abusive relationship to address the harms that flow from it. And for that we need more empathy, not less.

\textsuperscript{243} See supra note 29.
\textsuperscript{244} See supra notes 149–153 and accompanying text.
\textsuperscript{245} Calo, supra note 237, at 67–68 (discussing how perpetrators of digital abuse might suffer from mental-health issues).