THE YALE LAW JOURNAL FORUM
NOVEMBER 22, 2023

The Continued (In)visibility of Cyber Gender Abuse

Danielle Keats Citron

ABSTRACT. For too long, cyber abuse has been misunderstood and ignored. For everyday women and minorities, cyber abuse is unseen and unredressed due to invidious stereotypes and gender norms. The prevailing view is that cyber abuse is not "really real," though in rare cases authorities take it seriously. Justices of the U.S. Supreme Court demanded and received extra protection for themselves after facing online threats, but, in oral argument in *Counterman v. Colorado*, a case involving a man who sent a woman hundreds of unwanted, terrifying texts, members of the Court suggested that victims might be overreacting. In other words, protection for me (the powerful) but not for thee. The Court's ruling sent a clear message to victims that their speech and liberty do not matter as much as the speech of people whose words objectively terrorize them and gave law-enforcement officers and prosecutors additional reasons not to pursue cases. The Supreme Court has made matters much, much worse.

Empirical proof now exists that makes nonrecognition difficult to justify. Studies show that cyber abuse is widespread and has profound injuries, and that the abuse is disproportionately borne by women, who often have intersecting disadvantaged identities—hence, the moniker cyber gender abuse. After years of advocacy and scholarship, it pains me to acknowledge the continued invisibility of cyber gender abuse. Progress is possible if we recognize our failings and commit to structural reform. Internet exceptionalism must end for the businesses best situated to prevent destructive cyber gender abuse. Congress should also condition the immunity afforded content platforms on a duty of care to address cyber gender abuse and eliminate the legal shield for platforms whose business is abuse.

INTRODUCTION

Nina Jankowicz is a researcher and author specializing in state-sponsored disinformation.[1] In April 2022, the Biden Administration asked Jankowicz to lead a new group in the Department of Homeland Security (DHS) called the

1. I interviewed Ms. Jankowicz on December 12, 2022, and have continued to discuss the ongoing nature of the abuse she has been facing on the telephone and via Zoom.

Disinformation Governance Board.[2] Within hours of the Board's announcement, far-right media outlets denounced Jankowicz as the enemy of free speech.[3] Representative Lauren Boebert released a public statement saying Jankowicz was "a Russia hoax espousing radical who is on video singing and asking who she needs to have sex with to become famous and powerful."[4] On Sean Hannity's Fox News show, Representative Jim Jordan said that Jankowicz "will come after you" and Hannity accused her of spreading disinformation.[5] Over the next sixteen months, more than 250 broadcasts on Fox featured Jankowicz.[6]

In short order, Jankowicz faced a tsunami of cyber abuse. Doctored videos appeared online suggesting, falsely, that Jankowicz wanted hand-picked individuals to have the power to edit others' tweets.[7] Her home address, telephone number, and other contact information appeared on message boards, in tweets, and in online comments.[8] She was flooded with emails, texts, and voicemails from speakers threatening to kill her.[9] Jankowicz also discovered that her face had been morphed onto porn without her consent in a video circulating online.[10] At the time, she was nine months pregnant.[11] A private security consultant advised her "not to go to coffee shops, not to get gas alone."[12] Jankowicz and her husband were urged to leave their house, an impossibility given the stage of her

2. Shannon Bond, *She Joined DHS to Fight Disinformation. She Says She Was Halted by . . . Disinformation*, NPR (May 21, 2022, 5:00 AM EST), https://www.npr.org/2022/05/21/1100438703/dhs-disinformation-board-nina-jankowicz [https://perma.cc/5MBG-WC26]; Heidi Przybyla, *'A Surreal Experience': Former Biden 'Disinfo' Chief Details Harassment*, POLITICO (Mar. 8, 2023, 4:30 AM EST), https://www.politico.com/news/2023/03/08/former-biden-disinfo-chief-details-harassment-00085981 [https://perma.cc/W9YZ-P8PU].

3. *Id.*

4. Louis Casiano, *White House 'Disinformation Czar' Nina Jankowicz Makes TikTok Account Private*, FOX NEWS (May 3, 2022, 7:07 PM EDT), https://www.foxnews.com/politics/white-house-disinformation-nina-jankowicz-tiktok [https://perma.cc/2HPH-34UT].

5. Przybyla, *supra* note 2.

6. *Id.*

7. *Id.*

8. Stefano Kotsonis & Meghna Chakrabarti, *What Happened to Nina Jankowicz When Fox News Came for Her*, WBUR (May 15, 2023), https://www.wbur.org/onpoint/2023/05/15/nina-jankowicz-disinformation-how-fox-news-changed-her-life [https://perma.cc/EZ2A-3CY8]; Zoom Interview with Nina Jankowicz (Dec. 12, 2022).

9. Bond, *supra* note 2; Zoom Interview with Nina Jankowicz (Dec. 12, 2022).

10. E-mail from Nina Jankowicz to Danielle Citron (June 14, 2023) (on file with author).

11. Zoom Interview with Nina Jankowicz (Dec. 12, 2022).

12. *Id.*

pregnancy.[13] Jankowicz was terrified—even walking the dog seemed dangerous.[14]

In a month's time, the Biden Administration announced that it had decided to close the board. Although DHS gave Jankowicz the option of staying at the agency, she resigned.[15] Jankowicz and her family were left to face the abuse by themselves—she received no support from her former employer.[16] It took months before she returned to Instagram. To this day, she is careful about what she says and does on- and offline; she does not feel like she can express herself freely.[17] Jankowicz told *Politico* that her "entire career [had] be[en] lit on fire before [her] eyes."[18]

Public figures are not the only ones targeted; so are ordinary people. In May 2023, *USA Today* journalist Will Carless exposed a Telegram channel, "Project Mayhem," whose 1,500 followers participated in campaigns of abuse that they called "online raids." A prominent white supremacist who ran the channel coordinated attacks against Jewish college students, trans men, and Black individuals.[19] Perpetrators would "post a call to raid someone, usually identified by their social media accounts," and followers of the channel would flood the target's accounts with death threats, photographs of white power, and doxing.[20]

Cyber abuse has evolved. Jankowicz faced cyberstalking—the repeated targeting of someone online with a "course of conduct" that typically includes defamation, impersonation, threats, and nonconsensual disclosure of private information.[21] Cyberstalking can involve a destructive pattern or single instance of intimate-privacy violations, like the nonconsensual disclosure of authentic or

---

13. *Id.*

14. *Id.*

15. Zoom Interview with Nina Jankowicz (Dec. 12, 2022).

16. *Id.*

17. Kotsonis & Chakrabarti, *supra* note 8.

18. Przybyla, *supra* note 2; *see also* Will Carless, *They Were Flooded by Online Harassment and Hatred. They Didn't Know a Targeted Campaign Caused It*, USA TODAY (May 11, 2023, 7:13 PM ET), https://www.usatoday.com/story/news/nation/2023/05/03/telegram-channel-project-mayhem-paul-nicholas-miller/70171241007 [https://perma.cc/UTW6-V3KK] (describing an orchestrated campaign of online hate speech and harassment).

19. Carless, *supra* note 18.

20. *Id.*

21. *See* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 3 (2014). Cyberstalking involves the repeated targeting of someone with a "course of conduct"—multiple instances of abuse showing a continuity of purpose--that causes that person serious emotional distress and often the fear of physical harm and that would cause the reasonable person to suffer serious emotional distress or the fear of physical harm. *Id.*

manufactured intimate (nude or sexually explicit) images.[22] Victims are now being sexually harassed and groped in virtual-reality environments.[23] I affix *cyber* or *online* to describe such abuse to capture the varied and evolving ways that networked technologies can make abusive behavior more likely and exacerbate the damage.[24]

I began writing about cyber abuse in 2007.[25] From the start, commentators dismissed my concerns.[26] I was making much ado about nothing: criminal threats, cyberstalking, sexual invasions of privacy, and bias intimidation were "mean words."[27] The abuse was not recognized as a structural, gendered problem, but that was what was happening. As studies have made clear, women are more often the targets of cyberstalking, intimate-privacy violations, and sexual assault in virtual environments.[28] The Pew Research Center found that, in 2020, women were "more likely than men to report having been . . . stalked [online] (13% vs. 9%)."[29] Young women were "particularly likely" to experience sexual

22. *See, e.g.*, DANIELLE KEATS CITRON, THE FIGHT FOR PRIVACY: PROTECTING DIGNITY, IDENTITY, AND LOVE IN THE DIGITAL AGE 25-40 (2022).

23. *See, e.g.*, Mary Anne Franks, *Unwilling Avatars: Idealism and Discrimination in Cyberspace*, 20 COLUM. J. GENDER & L. 224, 226-27 (2011).

24. My book, *Hate Crimes in Cyberspace*, explored how some of the internet's key features — anonymity, mobilization of groups, and group polarization — make it more likely that people will act destructively and how other features, such as information cascades and Google bombs, enhance the destruction's accessibility, making it more likely to inflict harm. CITRON, *supra* note 21, at 56-72.

25. *See* CITRON, *SUPRA* NOTE 21; Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373 (2009) [hereinafter Citron, *Law's Expressive Value*]; Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61 (2009); Danielle Keats Citron, *Destructive Crowds: New Threats to Online Reputation and Privacy, Panel Presentation at the Yale Law School Reputation Economies in Cyberspace Symposium*, YOUTUBE (Jan. 9, 2008), http://www.youtube.com/watch?v=XVEL4RfN3uQ [https://perma.cc/AP93-BVD7].

26. *See* CITRON, *supra* note 21, at 73-80.

27. *See id.*; *see also* Scott H. Greenfield, *Slander, Talk Radio, and Cyber Civil Rights*, SIMPLE JUST. (Apr. 26, 2009), https://blog.simplejustice.us/2009/04/26/slander-talk-radio-and-cyber-civil-rights [https://perma.cc/V2A9-U38Q] (describing cyberstalking as "people saying mean things").

28. *See, e.g.*, Amanda Lenhart, Michele Ybarra, Kathryn Zickuhr & Myeshia Price-Feeney, *Online Harassment, Digital Abuse, and Cyberstalking in America*, DATA & SOC'Y RSCH. INST. & CTR. FOR INNOVATIVE PUB. HEALTH RSCH. 4 (2016), https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf [https://perma.cc/MA57-S9KA]. Many victims have more than one marginalized identity. *See* CITRON, *supra* note 22, at 39-40.

29. Emily A. Vogels, *The State of Online Harassment*, PEW RSCH. CENTER (Jan. 13, 2021), https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment [https://perma.cc/R8ZF-4SHC]. Further, fifty-one percent of LGBTQ people reported facing severe online abuse as compared to twenty-three percent of straight adults. *Id.* Black and Hispanic individuals are more likely to face severe online abuse due to their race. *Online Hate*

harassment online; "[f]ully 33% of women under 35 say they have been sexually harassed online, while 11% of men under 35 say the same."[30] Another nationwide study found that about one in eight adult social media users have been threatened with or been the victim of the nonconsensual sharing of private, sexually explicit images or videos; that women were approximately 1.7 times more likely to be victimized than men; and that men were the primary perpetrators of the abuse.[31] When victims appear to be female, nonwhite, or LGBTQ (and often a combination of disadvantaged identities), cyber abuse is suffused with misogynistic, racist, and homophobic invective.[32]

Then, too, cyber abuse was suffused with gender stereotypes. Perpetrators of such abuse cast women as sexual objects deserving to be raped; as vectors for sexually transmitted disease; and as prostitutes.[33] Women were told to stay offline.[34] Victims were dismissed as hysterical "drama queens" who were too frail for public engagement.[35] The abuse and the public's reaction suggested that "online spaces constituted male turf."[36] Given the gendered nature of the abuse, it is more aptly described as *cyber gender abuse*.[37]

Society, as this Essay will argue, still refuses to recognize cyber gender abuse as wrongful, even though empirical proof shows the damage that it causes. As studies show, female victims are plagued with severe and lasting fear, worry, and

and Harassment: The American Experience, ANTI-DEFAMATION LEAGUE (Feb. 11, 2019), https://www.adl.org/resources/report/online-hate-and-harassment-american-experience [https://perma.cc/Y4F3-UJYA].

30. Vogels, *supra* note 29.

31. Asia A. Eaton, Holly Jacobs & Yanet Ruvalcaba, *2017 Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration: A Summary Report*, CYBER C.R. INITIATIVE 11-12, 15 (June 2017), https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf [https://perma.cc/BLP2-CQRM].

32. Citron, *Cyber Civil Rights*, *supra* note 25, at 64-66.

33. Citron, *Law's Expressive Value*, *supra* note 25, at 389.

34. *Id.* at 380 (collecting comments, which included "who let this woman out of the kitchen?" and "why don't you make yourself useful and go have a baby?").

35. *Id.* at 396.

36. *Id.* at 390, 396.

37. Citron, *Cyber Civil Rights*, *supra* note 25, at 74-75.

pain.[38] Women's speech is silenced.[39] A report issued by Data and Society in 2016 explained that "younger women are the group most likely to self-censor to avoid potential online harassment: 41% of women ages 15 to 29 self-censor[ed], compared with 33% of men of the same age group and 24% of internet users ages 30 and older (men and women)."[40]

Cyber gender abuse also wrecks victims' reputations and careers.[41] Employers treat Google searches of people's names as part of their resumes.[42] Because online searches are often the first things that clients and coworkers see about someone, employers are reluctant to hire people with damaged online identities.[43] Job applicants are not usually given the opportunity to address cyber

38. NICOLA HENRY, CLARE MCGLYNN, ASHER FLYNN, KELLY JOHNSON, ANASTASIA POWELL & ADRIAN J. SCOTT, IMAGE-BASED SEXUAL ABUSE: A STUDY ON THE CAUSES AND CONSEQUENCES OF NON-CONSENSUAL NUDE OR SEXUAL IMAGERY 7-15 (2021) (describing the findings from a study on "image-based sexual abuse"); Eaton, Jacobs & Ruvalcaba, *supra* note 31, at 23-24 (demonstrating heightened negative mental-health outcomes and higher levels of psychological problems as a result of nonconsensual porn); Nicola Henry & Anastasia Powell, *Beyond the 'Sext': Technology-Facilitated Sexual Violence and Harassment Against Adult Women*, 48 AUSTL. & N.Z. J. CRIMINOLOGY 104, 113-14 (2015); Asher Flynn, Nicola Henry & Anastasia Powell, *More than Revenge: Addressing the Harms of Revenge Pornography*, MONASH UNIV., LA TROBE UNIV. & RMIT UNIV. 4-5 (2016) (describing the findings from a study on "image-based sexual exploitation" and explaining the harms caused by the nonconsensual distribution of images, including stalking, humiliation, and loss of employment).

39. *See* Jonathon W. Penney, *Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study*, 6 INTERNET POL'Y REV. 1, 19 (2017) (finding that women are statistically more chilled in their speech and engagement when they are targeted with online abuse).

40. Lenhart, Ybarra, Zickuhr & Price-Feeney, *supra* note 28, at 4.

41. CITRON, *supra* note 22, at 36, 41-45; CITRON, *supra* note 21, at 40; Flynn, Henry & Powell, *supra* note 38, at 5 (explaining the harms caused by the nonconsensual distribution of images, including stalking, humiliation, and loss of employment).

42. CITRON, *supra* note 21, at 8-10.

43. *Id.*; Danielle Keats Citron, *Presidential Privacy Violations*, 2022 U. ILL. L. REV. 1913, 1915 (2022) (documenting the obliteration of careers of FBI officials due to DOJ and President Trump's cyberstalking and intimate-privacy violations); Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 842 (2022) ("The emotional toll of identity theft can adversely affect victims' work and relationships."); Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805, 1813 (2010); Citron, *Cyber Civil Rights*, *supra* note 25, at 80. A 2020 study found that a staggering ninety-eight percent of employers conduct background research about candidates online to know more about them. Kelsey McKeon, *Five Personal Branding Tips for Your Job Search*, MANIFEST (Apr. 28, 2020), https://themanifest.com/digital-marketing/5-personal-branding-tips-job-search [https://perma.cc/RK6Q-6Q73]. A national study of hiring managers and human resource professionals conducted in 2017 found that seventy percent of employers surveyed conduct online searches for prospective hires; fifty percent said that they assess whether candidates have a "professional online persona." *Number of Employers Using Social Media to Screen Candidates at All-Time High, Finds Latest CareerBuilder Study*, CAREERBUILDER (June 15, 2017), http://press.careerbuilder.com/2017-06-15-Number-of-

abuse prominent in searches of their names.[44] No matter how qualified the candidate with a damaged online identity is, employers avoid the risk involved in hiring them.[45]

This Essay explores society and law's continued nonrecognition of cyber gender abuse.[46] Cyber gender abuse is dismissed as innocuous or the victims' fault. That the abuse happens *online* provides further reasons for institutional actors to ignore it. Law enforcement insists that because cyber gender abuse involves words and images "out there in cyberspace," as if that differs from real space, victims can solve the problem by ignoring perpetrators' posts. Tech companies have taken a different, yet complimentary tack by arguing that rather than irrelevant, online speech is essential to public discourse. Regulating cyber abuse, they say, would endanger free speech, even though law's protections would free victims to speak.[47] Victims have no legal recourse against content platforms that are best positioned to minimize the damage. A federal law passed in 1996 provides an iron-clad immunity to platforms for illegal conduct, even when platforms solicit and profit from that conduct.[48] The drafters of that statute hoped that the immunity would incentivize "Good Samaritan" self-monitoring, but the law's overbroad judicial interpretation has turned into a license to abuse.

Just when it seemed that the problem of nonrecognition could not get worse, the U.S. Supreme Court joined the fray. This past Term, at oral argument for a case about the constitutionality of a cyberstalking conviction, some Justices laughed when discussing the plight of a woman who over two years received *hundreds* of menacing text messages from a stranger who she repeatedly blocked but who kept evading her blocking efforts and invading her inbox.[49] Remarks from the bench made light of isolated messages and suggested that people were "increasingly sensitive."[50] The Court's decision in that case, *Counterman v.*

Employers-Using-Social-Media-to-Screen-Candidates-at-All-Time-High-Finds-Latest-CareerBuilder-Study [https://perma.cc/DZ6E-AR6C].

44. CITRON, *supra* note 21, at 8.

45. *Id.*

46. Dr. Mary Anne Franks, Dr. Holly Jacobs, and I founded the Cyber Civil Rights Initiative (CCRI) a decade ago to advocate on behalf of victims of intimate-privacy violations and cyberstalking. Our mission, then and now, is to protect "civil rights and civil liberties" in the digital age. For more information, see *History*, CYBER C.R. INITIATIVE, https://cybercivilrights.org/about [https://perma.cc/3KK2-AYM7] (discussing the story of our founder Dr. Holly Jacobs).

47. Danielle Keats Citron & Jonathon W. Penney, *When Law Frees Us to Speak*, 87 FORDHAM L. REV. 2317, 2329-32 (2019).

48. *Id.* at 2331-2333.

49. Transcript of Oral Argument at 53-57, Counterman v. Colorado, 600 U.S. 66 (2023) (No. 22-138).

50. *Id.* at 53-57, 65, 81-82.

Colorado,[51] dealt a serious blow to cyberstalking victims in finding that the First Amendment's chilling-effects doctrine requires heightened mental state of recklessness for threats, which would show that the defendant consciously disregarded the substantial risk that his words would be taken as a serious threat of violence.[52] The ruling failed to acknowledge that cyberstalking and threat laws protect victims' expressive autonomy. Victims' speech and liberty did not matter as much as the speech of people whose words are objectively terrorizing. Law enforcement and prosecutors have even more reason now to ignore cyberstalking complaints because those cases are now tougher to prove. The Supreme Court has made matters much worse.

We can and must act now. Societal and legal nonrecognition tells victims that they cannot count on institutions to help them. They get the message that their suffering does not matter. And an even more insidious message is sent to *perpetrators*: cyber gender abuse is unlikely to cost them anything even as it costs victims everything. Now that the Supreme Court has further set back victims' efforts to garner the support of the criminal law, we need society and law to recognize cyber gender abuse as wrongful and to see and minimize the harm it inflicts.

With this Essay, I hope to reignite the discussion around cyber gender abuse so that the wrongs perpetrated and the harms inflicted do not continue to be brushed aside. Restarting this conversation is even more urgent after the *Counterman* announcement that objectively terrifying abuse must be tolerated. This Essay lays out a reform agenda centered on the crucial structures enabling and profiting from the abuse—the content platforms. Part I highlights the never-ending dismissal of cyber gender abuse. Then, Part II advances the discussion by showing how the recent Supreme Court in *Counterman v. Colorado* overlooked the damage inflicted by cyberstalking, including the silencing of victims. Finally, Part III concludes with an overview of necessary reforms. The era of no liability for content platforms needs to pass. It is time for law to intervene for content platforms that do not take reasonable steps to address cyber gender abuse. It is also time for attorneys to play a role in helping victims. Right now, perpetrators think that online assaults are costless because law enforcement does not knock on their door and because victims mostly cannot afford to hire counsel to sue them. To change that impression and victims' reality, bar associations should encourage lawyers and law firms to devote part of their pro bono practice to cyber-gender-abuse cases.

---

51. 600 U.S. 66 (2023).

52. *Id.* at 69-70.

I. SHINING THE LIGHT ON THE TRIVIALIZATION OF CYBER ABUSE

The trivialization of harms that disproportionately impact women is not new.[53] This Part begins by connecting the historical trivialization of gendered harms to the nonrecognition of cyber gender abuse, emphasizing enduring similarities, as well as differences, that make getting the public's attention even tougher. This Part then shows how law enforcement and content platforms fail to recognize and address cyber abuse and worse, how some encourage it. The law also has failed us by immunizing from liability companies that solicit, encourage, or leave up cyber gender abuse.

A. Patterns of Nonrecognition

Throughout U.S. history, society has dismissed women's suffering as innocuous. Recall that until the early-to-mid 1970s, society regarded workplace sexual harassment as harmless flirting.[54] Employers once routinely told women to switch supervisors or get new jobs if sexual harassment at work was too difficult to bear.[55] At work, men were free to engage in sexual harassment because it was "a perk for men to enjoy"[56] Another recurring theme was that women had only themselves to blame for their suffering. Commentators argued that lawsuits would suffocate workplace expression and impair (male) worker camaraderie.[57] In the domestic-violence context, "judges and caseworkers similarly treated battered women as the responsible parties rather than their abusers."[58] Courts and police refused to arrest domestic batterers because the home was sacred, and arrests would break up marriages.[59]

---

53. ROBIN WEST, CARING FOR JUSTICE 96-97 (1997). As Robin West has shown, criminal law historically addressed gender-specific harms only to the extent that they resembled harms suffered by men. *Id.* at 138-40. Rape law was clearest and most addressed when attacks resembled nonsexual physical attacks that men suffered and feared, that is, attacks by strangers. *Id.* at 140 (noting that "[r]apes committed by husbands upon wives, or by boyfriends upon girlfriends, or by johns on prostitutes" were "underregulated"). Nineteenth-century tort law followed a similar pattern by refusing to recognize claims mainly pursued by women, like emotional distress claims. Martha Chamallas & Linda K. Kerber, *Women, Mothers, and the Law of Fright: A History*, 88 MICH. L. REV. 814, 816 (1990).

54. Citron, *Law's Expressive Value*, *supra* note 25, at 393.

55. *See* CITRON, *supra* note 21, at 80-82.

56. Citron, *Law's Expressive Value*, supra note 25, at 394.

57. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 124-25 (2000).

58. CITRON, *supra* note 21, at 82.

59. *Id.* at 83.

These themes recur in the cyber-gender-abuse context. Law enforcement trivializes the abuse that women face in similar ways to how society dismissed women's abuse at work and at home. Police officers accuse female victims of making a big deal out of nothing and tell them to ignore the abuse.[60] Abuse is a feature, not a bug, for sites devoted to nonconsensual intimate images. Even mainstream content platforms have said that cyber gender abuse is part of the rough and tumble of networked environments. In turn, tech lobbyists repeat the view that regulation would chill perpetrators' speech, without regard to how the abuse silences victims.[61]

The trivialization of the past does not exactly mirror that of the present. That the abuse happens *online* provides additional reasons to dismiss it. The view is that cyber abuse is not as harmful as physical assault or in-person intimidation. Words and images cannot harm people in the same way as physical actions, they say.[62] This reaction — a variation of "sticks and stones may break my bones, but words will never hurt me" — misses the way that networked technologies can *exacerbate*, not lessen, the abuse.[63] Words and images posted online are viewable, searchable, and salient to anyone, anywhere; strangers near and far can join and further propagate the abuse. The mean words of the schoolhouse yard — ephemeral and contained — are paltry by comparison.

The gendered impact and the way that networked technologies magnify the destruction, taken together, make clear that we need to tackle societal nonrecognition of cyber gender abuse on its own terms. The necessity of a cyber-gender-abuse-specific strategy is exacerbated by the law's differential treatment of content platforms and physical workplaces, as this Essay explores in Part III.[64]

---

60. *Id.*; CITRON, *supra* note 22, at 78-81.

61. *See* MARY ANNE FRANKS, THE CULT OF THE CONSTITUTION 164 (2019).

62. CITRON, supra note 21, at 74 (noting commentators' view that "unlike 'real rape,' words and images on a screen cannot really hurt anyone"). This recalls the response to Catharine A. MacKinnon's groundbreaking scholarship on workplace sexual harassment — that courts should not recognize claims under Title VII for sex discrimination if the harassment involved is "only words." *See* CATHARINE A. MACKINNON, ONLY WORDS 58-62 (1996) (arguing that verbal harassment is itself a form of sexual abuse). MacKinnon and advocates showed that hostile sexual environments were tantamount to conduct that changed the terms and conditions of the workplace. Courts in the late 1970s and early 1980s came around to MacKinnon's view and recognized such claims. Citron, *Law's Expressive Value*, *supra* note 25, at 407-08. The Supreme Court views workplace sexual harassment as proscribable conduct. Wisconsin v. Mitchell, 508 U.S. 476, 487 (1993) (pointing to Title VII as a civil-rights law that does not infringe upon free speech because it proscribes unequal treatment of individuals in tangible ways, not the content of a defendant's expression).

63. *See* CITRON, *supra* note 21, at 4-6, 56-72.

64. *See* Mary Anne Franks, *Sexual Harassment 2.0*, 71 MD. L. REV. 655, 657 (2012).

B. Societal Refusal to Recognize Cyber Abuse as Wrongful

In the present, as in the past, key institutions have failed to combat abuses that disproportionately impact women. Law enforcement has dismissed cyber abuse as unworthy of attention. The tech industry's response is also a crucial part of society's nonresponse. To put the response of the major tech companies into perspective, I will show that thousands of sites do not just ignore cyber gender abuse, they make a business of nonconsensual intimate images. While some major tech companies have finally taken steps to ban cyberstalking and intimate-privacy violations, others are regrettably repeating their early pattern of nonrecognition in response to virtual sexual assaults.

1. Law Enforcement's (Non)response & Worse

Much as police officials dismissed domestic violence and sexual assault reported by women (until advocates, courts, and policymakers helped begin to change those attitudes in the late 1970s and 1980s), law enforcers refuse to recognize cyber gender abuse as wrongful, even though laws on the books often criminalize it.[65] Police officers insist that cyber gender abuse is "no big deal."[66] For example, officers in Florida told Cyber Civil Rights Initiative (CCRI) founder Holly Jacobs, whose nude images were posted online without consent, that her case involved a "civil" matter, even though the state criminalized cyber harassment.[67] Officers say that victims should feel flattered by the attention. A police officer in New York told a woman that she "should feel good about appearing on 'cum tribute' sites that showed videos of men masturbating to her nude photo, which was posted without her permission."[68] Local police told journalist Amanda Hess, who was repeatedly and graphically threatened on Twitter, that she could avoid the abuse by not using the site.[69]

Law enforcers engage in a game of jurisdictional hot potato, leading victims to run in circles. Police officers tell victims that another jurisdiction is best suited to help them. Victims then go to that jurisdiction; officers there pass victims off to yet another jurisdiction.[70] This cycle repeats until there is no one left to

---

65. CITRON, *supra* note 21, at 83-85.

66. CITRON, *supra* note 22, at 77.

67. CITRON, *supra* note 21, at 85-87.

68. CITRON, *supra* note 22, at 77.

69. CITRON, *supra* note 21, at 84.

70. *See infra* text accompanying note 73.

recommend.[71] Victims give up, having wasted countless hours of time. Victims get the message that law enforcement will not help them.

Consider how officers treated Kara Jefts, who is an art historian and museum curator. Jefts went to law enforcement with screenshots of her ex-boyfriend's countless posts displaying her nude images alongside accusations that she had a sexually transmitted disease, copies of emails and texts that her ex sent to her mother and grandmother with her nude images, and samples of the thousands of e-mails that her ex sent her threatening rape and death.[72] Officers said that none of it was serious—"images could not hurt her," so she should "just ignore it"—and always ended their discussions by sending Jefts to other jurisdictions. She went to law-enforcement precincts in three different New York counties—Schenectady, Troy, and Albany—to no avail.[73] In every encounter, Jefts tried to convince officers to take her case seriously.[74] She explained that she could not ignore the posts with her nude images and accusations that she had a sexually transmitted disease (which she did not) because they appeared in searches of her name, which meant that she had to explain them to employers, friends, and dates.[75] Officers in New York and Illinois—where Jefts eventually moved—refused to help her.[76]

Even high-profile individuals have had little success with law enforcement. In 2014, Brianna Wu, founder of the video game company Giant Spacekat,

---

71. This was a theme of our recent convening at the White House for the Gender Policy Council. On April 26, 2023, Dr. Mary Anne Franks and I, on behalf of CCRI, joined together with victims of cyberstalking and intimate-privacy violations as well as victims' advocates to brief state lawmakers. This theme was raised again and again throughout the meeting. *See Press Release, White House, Readout of White House State Legislative Convening on Non-Consensually Distributed Intimate Images* (Apr. 26, 2023) https://www.whitehouse.gov/briefing-room/statements-releases/2023/04/26/readout-of-white-house-state-legislative-convening-on-non-consensually-distributed-intimate-images [https://perma.cc/8EXU-QXS8].

72. Zoom Interview with Kara Jefts (Aug. 14, 2020).

73. *Id.*

74. *Id.*

75. *Id.*

76. *Id.* After years of wrestling with the abuse, Jefts shared her story with the media and advocated for change. Charlotte Alter, *'It's Like Having an Incurable Disease': Inside the Fight Against Revenge Porn*, TIME (June 13, 2017, 5:00 AM EDT), https://time.com/4811561/revenge-porn [https://perma.cc/2N58-KNL5]. When she came forward, CCRI expressed deep appreciation for her bravery and advocacy. End Revenge Porn, FACEBOOK (June 13, 2017, 1:52 PM), https://www.facebook.com/EndRevengePorn/posts/incredibly-proud-of-kara-jefts-a-victim-of-nonconsensual-porn-ncp-who-went-publi/1461724490554192 [https://perma.cc/KZ9T-2SKL].

denounced vicious online attacks on fellow female game developers.[77] Perpetrators responded to Wu's criticism with a vicious campaign of cyberstalking.[78] People tried to hack Wu's studio.[79] They doxed and threatened her. One poster wrote, "I've got a K-bar and I'm coming to your house so I can shove it up your ugly feminist cunt."[80] Attackers "shot videos wearing skull masks and showing viewers knives they said they planned to murder [her] with."[81] Over 180 death threats filled her inbox.[82] Wu and her husband left their home because they did not feel safe.[83]

Even though Wu's case garnered attention from major media outlets, federal law enforcement provided little help. After years of waiting, Wu tried to get to the bottom of the FBI's nonresponse and sent FOIA requests for the records in her case.[84] The highly redacted report that she received showed that the "FBI didn't take the investigation very seriously and let off harassers with simple warnings."[85] The FBI did not follow up on many of the leads that Wu *gave* to agents.[86] Wu explained: "[S]even months into [#Gamergate], we got an email from the FBI saying they'd never read anything we'd sent them. They asked us to send them a hard drive with the information on it and we did. We got a read receipt, and a few weeks later it was mailed back to us. NONE OF THAT MADE IT INTO THE REPORT."[87] Law-enforcement officers interviewed people who

77. Brianna Wu, *I Wish I Could Tell You It's Gotten Better. It Hasn't.*, N.Y. TIMES (Aug. 15, 2019), https://www.nytimes.com/interactive/2019/08/15/opinion/brianna-wu-gamergate.html [https://perma.cc/BYP2-LM5F].

78. *Id.*

79. *Id.*

80. Keith Stuart, *Brianna Wu and the Human Cost of Gamergate: 'Every Woman I Know in the Industry Is Scared,'* GUARDIAN (Oct. 17, 2014, 2:02 PM EDT), https://www.theguardian.com/technology/2014/oct/17/brianna-wu-gamergate-human-cost [https://perma.cc/7LVN-B7NG].

81. Wu, *supra* note 77.

82. Dean Takahashi, *Brianna Wu Appalled at FBI's #GamerGate Investigative Report*, VENTUREBEAT (Jan. 29, 2017, 9:33 AM), https://venturebeat.com/games/brianna-wu-appalled-at-fbis-gamergate-investigative-report [https://perma.cc/Q9JW-ZLK5].

83. Stuart, *supra* note 80.

84. Takahashi, *supra* note 82.

85. *Id.*

86. A.E. Osworth, *Brianna Wu Is Here, Queer and Running for Congress in Massachusetts*, AUTOSTRADDLE (Feb. 2, 2017), https://www.autostraddle.com/brianna-wu-is-here-queer-and-running-for-congress-in-ma-8-367665 [https://perma.cc/JB3C-QEY2].

87. Takahashi, *supra* note 82.

admitted that they had threatened Wu,[88] but, ultimately, the report concluded that there were no actionable leads or subjects and closed the investigation.[89]

Law enforcement's nonrecognition of cyber abuse "leave[s] an indelible, painful mark."[90] Victims internalize the view that cyber abuse is their fault.[91] They feel ashamed and embarrassed, as Jefts did.[92] They lose faith in law enforcement, just as Jefts and Wu did.[93] After reporting abuse and getting no help, victims feel "more alone, more afraid, and more embarrassed than [they'd] felt when [they] first walked into the precinct."[94] The message to other victims is that it is not worth reporting cyber abuse because officers will not take it seriously.[95]

Law enforcement's refusal to recognize cyber gender abuse results in the underenforcement of criminal law. Thanks to the advocacy of CCRI and the tireless work of Mary Anne Franks, forty-eight states, the District of Columbia, and Guam have laws criminalizing the nonconsensual posting of intimate images.[96] Most states and federal law criminalize cyberstalking and electronic harassment.[97] Those laws, however, are rarely invoked, which was a theme of our discussions at the White House Gender Policy Council with state lawmakers. Many victims are reluctant to report cyber gender abuse because they suspect that law enforcers will ignore complaints; sadly, they are not wrong.[98] With scant law-

88. *Id.* Victims' advocates refer to this as the "some other dude" defense, which agents in Brianna Wu's case seemingly took at face value. Surely, every defendant says that "it was not me, it was someone else." One can imagine that this defense is not simply accepted in nongendered cases like bank robberies or financial fraud.

89. *Id.*

90. CITRON, *supra* note 22, at 78.

91. *See id.* at 80-81; *see also* Interview with "Joan" (May 3, 2019) (explaining that she blamed herself when a hotel employee posted videos of her showering and going to the bathroom in her hotel room to porn websites).

92. Interview with Kara Jefts, *supra* note 72.

93. *Id.*; Takahashi, *supra* note 82.

94. *Id.*

95. *See* CITRON, *supra* note 22, at 81 (noting studies showing that seventy-five percent of victims of nonconsensual intimate imagery reported taking no steps to contact law enforcement, twenty-nine percent of victims felt that reporting would not change anything, twenty-two percent simply did not know what to do, and eighteen percent felt too ashamed to file a report); Citron, *Law's Expressive Value*, *supra* note 25, at 402.

96. CITRON, *supra* note 22, at 196.

97. CITRON, *supra* note 21, at 104.

98. *See* CITRON, *supra* note 22, at 80-81; CITRON, *supra* note 21, at 83 (describing a survey showing that the majority of stalking victims failed to contact police and that seventeen percent believed the police would not help them because they would not take it seriously or because they would blame them for the abuse).

enforcement activity, perpetrators think that their behavior is consequence-free.[99]

2. *Encouraged Rather than Wrongful: Nonconsensual-Intimate-Imagery Sites*

Societal nonrecognition of cyber gender abuse as *wrongful* is evident in the operation of sites devoted to nonconsensual intimate images. Site operators urge visitors to post nonconsensual intimate images as if a game were afoot.[100] Without remorse, sites explicitly blame victims, saying that "[i]f anyone is at fault, it is the subject of the images, whose poor choices enabled the display."[101] With that encouragement and law enforcement's inattention, perpetrators get the message that their behavior is acceptable, fun, and consequence-free.

An ecosystem of sites solicits and profits from cyber gender abuse. More than 9,500 sites host user-provided nonconsensual intimate images, including up-skirt, down-blouse, and deepfake sex videos, and authentic intimate images.[102] Sites pair women's (real or fake) nude or sexually explicit photographs with their college crests and information about their friends and classmates.[103] Images mostly feature everyday women rather than celebrities, and they are less explicit than pornography; the draw to these sites is that the women featured have not consented to the posting of their images.[104]

Nonconsensual intimate imagery is depicted as normal business. Sites charge subscribers "monthly fees, collecting ad revenue from people's clicks, or amassing personal data, which they can sell."[105] In 2018, the Candid Forum had more than 200,000 subscribers paying $19.99 a month to view up-skirt and

---

99. *See* CITRON, *supra* note 22, at 76 (discussing the findings from an Australian e-Safety survey of perpetrators of intimate-privacy violations); Eaton, Jacobs & Ruvalcaba, *supra* note 31, at 22 (discussing survey of intimate-privacy perpetrators that showed a top factor that would have stopped perpetrators was greater legal consequences).

100. CITRON, *supra* note 22, at 72.

101. *Id.*

102. *Id.* at 71-72.

103. *Id.* at 74.

104. *See* Amanda Marcotte, *'The Fappening' and Revenge Porn Culture: Jennifer Lawrence and the Creepshot Epidemic*, DAILY BEAST (Apr. 14, 2017, 2:53 PM ET), https://www.thedailybeast.com/the-fappening-and-revenge-porn-culture-jennifer-lawrence-and-the-creepshot-epidemic [https://perma.cc/7MK2-B4LT]; Amanda Marcotte, *"Men's Rights" and "Revenge Porn" Sites Seethe with Anger over Women's Autonomy*, TRUTHOUT (Dec. 18, 2013), https://truthout.org/articles/mens-rights-and-revenge-porn-sites-seethe-with-anger-over-womens-autonomy [https://perma.cc/FD5D-3BJH].

105. CITRON, *supra* note 22, at 71-72.

down-blouse images from all over the world.[106] Most sites are hosted in countries like the United States where the risk of liability for privacy invasions is low.[107]

Nonconsensual-intimate-image sites market themselves as "fun" places to post and view women's nude, partially nude, or sexually explicit photos—nothing problematic happening here.[108] The *Candid Forum*'s front page says: "Sexy up-skirts have never been easier to capture thanks to cell phone cameras, so we're getting more submissions than ever."[109] As I wrote in *The Fight for Privacy*:

> Popular nonconsensual intimate image sites have hundreds upon hundreds of posters and commenters who treat women's bodies as theirs to view, trade, and insult. Women are referred to as "that ass on the right," "fuckable tits," and "desperate skinny bitches." Posters invoke stereotypes in labeling photos. A down-blouse thread on a hidden camera site had more than 150,000 videos with titles like "Very busty white girl spotted on Japan street with jiggling big boobs," "Black woman with dreadlocks in bikini," and "Sexy Asian Teen."[110]

As journalist Amanda Hess wrote of nonconsensual-intimate-image sites: "This is a world beyond humiliation."[111] These sites normalize cyber gender abuse by suggesting that it is entertainment to share, comment on, and display the intimate images of women who do not want or expect their nude images to be shared. These sites effectively tell perpetrators that it is acceptable to treat women as sexual objects and to treat them as "tits" and "asses" deserving of violation. They make cyber gender abuse seem like a typical pastime for men, rather than wrongful and harmful abuse. They suggest that only posters' expression matters—though posts actually involve women's coerced sexual expression and ultimately their silencing. These sites are "structures that permit the violation of intimate privacy" and other forms of cyber gender abuse.[112]

---

106. *Id.* at 72.

107. *Id.*

108. *See id.*

109. *Id.*

110. *Id.* at 73.

111. *Id.* at 75.

112. *Id.* at 76. *See also* SARA AHMED, LIVING A FEMINIST LIFE 24 (2017) (observing that many women experience public spaces as fraught with danger of sexual violence and internalize the message that they did something wrong if someone sexually violates them); IRIS MARION YOUNG, INTERSECTING VOICES: DILEMMAS OF GENDER, POLITICAL PHILOSOPHY, AND POLICY 27-29 (1997) (explaining that bodies, artifacts, and social spaces are "flooded with gender codes").

Studies show that these messages of normalization, blame, and permission have sunk in. Responding to a 2017 nationwide survey, 159 of 3,044 adults admitted to having shared another person's sexually explicit images or video without that person's permission.[113] Of those individuals, 104 were men and 55 were women.[114] Seventy-nine percent of the 159 individuals said that they wanted to share the images with friends; four percent found it "fun" or "funny" to share the images; seven percent said that it made them feel good; and four percent said that they did it to garner "upvotes/likes/comments/retweets etc. on the internet."[115] Eleven percent said that they did it because they were upset with the person in the image for another reason.[116] Most of those individuals said that they would not have shared the image if they knew they could face criminal consequences for their actions.[117] Nonconsensual-intimate-image sites perpetuate the sense that posters have done nothing wrong and that women only have themselves to blame.

3. Tech Companies' Nonresponse to Sexual Assault and Harassment in Virtual-Reality Environments

What about the major tech companies like Google, Meta, Microsoft, and Twitter (now known as X)? In the early years (2009-2014), it was difficult to convince platforms to address cyber gender abuse.[118] Consider my experience advising Twitter. In 2009, when I first began working with Twitter's Del Harvey (then the only safety employee), the company refused to do anything about threats, harassment, and intimate-privacy violations.[119] Harvey tried to push the C-suite into action, but nothing happened.[120] According to the C-suite, Twitter

---

113. Eaton, Jacobs & Ruvalcaba, *supra* note 31, at 11.

114. *Id.* at 15.

115. *Id.* at 19.

116. *Id.*

117. *Id.* at 22.

118. On behalf of CCRI, Franks and I have worked with social-media companies on their speech policies. I began that work in 2009 with Twitter, and then with the founding of CCRI in 2013, Franks and I did that work together with Twitter, Facebook, Google, and other companies. The staff with whom we worked at every company genuinely understood and cared about cyber gender abuse. The C-suite executives had to be convinced because it would cost them money, and convincing them was no easy task. I discuss some of that work in my scholarship. *See* CITRON, *supra* note 22, at 170-73; Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1955-58 (2019).

119. *See* Danielle Keats Citron & Hany Farid, *This Is the Worst Time for Donald Trump to Return to Twitter*, SLATE (Nov. 20, 2022, 7:59 PM), https://slate.com/technology/2022/11/trump-returning-to-twitter-elon-musk.html [https://perma.cc/X6RT-BMHP].

120. *See id.*

represented the "free speech wing of the free speech party."[121] That meant it would address only spam, copyright violations, and impersonations.[122] It took the convergence of key events to change matters — namely, the appointment of a new CEO (Jack Dorsey) and bad press after #GamerGate (including Wu's cyberstalking). The company switched course and banned cyberstalking, threats, and nonconsensual intimate imagery.[123]

Yet the impulse for societal nonrecognition has not abated. An emerging problem — sexual harassment in virtual reality (VR) — shows that tech companies are following the same script. VR technologies enable immersive experiences in which the user experiences an avatar's experiences as their own.[124] Participants can wear haptic vests, "which relay[] sensations through buzzes and vibrations."[125] And VR environments are poised to become even more immersive: researchers at Carnegie Mellon have "developed a VR attachment for a headset that sends ultrasound waves to the mouth, allowing people to feel sensations on the lips and teeth."[126] Meta's Mark Zuckerberg anticipates "a metaverse where people can be fitted with full-body suits that let them feel even more sensations."[127]

---

121. *Id.*

122. *See id.*

123. *See id.*; Willie Grace, *Twitter Beefs Up Anti-Troll Tools*, HOUS. STYLE MAG. (Dec. 2, 2014, 4:24 PM), http://stylemagazine.com/news/2014/dec/02/twitter-beefs-anti-troll-tools [https://perma.cc/TU97-7FHN]; *see also* Will Oremus, *When Twitter Blows the Whistle*, SLATE (July 19, 2018, 12:25 PM), https://slate.com/technology/2018/07/twitters-vijaya-gadde-on-its-approach-to-free-speech-and-why-it-hasnt-banned-alex-jones.html [https://perma.cc/QM2Q-X268] (interviewing Twitter's Chief of Trust and Safety about the company's approach to free speech); Sherisse Pham, *Twitter Tries New Measures in Crackdown on Harassment*, CNN (Feb. 7, 2017, 9:57 PM ET), https://money.cnn.com/2017/02/07/technology/twitter-combat-harassment-features [https://perma.cc/9A5Y-GKAL] (describing safety features that Twitter added to combat online harassment).

124. *See* Katherine Singh, *There's Not Much We Can Legally Do About Sexual Assault in the Metaverse*, REFINERY29 (June 9, 2022, 1:42 PM), https://www.refinery29.com/en-us/2022/06/11004248/is-metaverse-sexual-assault-illegal [https://perma.cc/FE54-9C7F]. "[Virtual Reality (VR)] technologies create an immersive, 3D, computer-generated, artificial environment, which replicates either the physical world or an imaginary world . . . . VR replaces the user's physical reality with a simulated one with realistic sounds, images, and other sensations." LING ZHU, CONG. RSCH. SERV., R47224, THE METAVERSE: CONCEPTS AND ISSUES FOR CONGRESS 11 (2022) (footnote omitted).

125. Sheera Frenkel & Kellen Browning, *The Metaverse's Dark Side: Here Come Harassment and Assaults*, N.Y. TIMES (Dec. 30, 2021), https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html [https://perma.cc/92MR-88ES].

126. Amanda Hoover, *The Metaverse Has a Sexual Harassment Problem and It's Going to Get Worse*, MORNING BREW (June 14, 2022), https://www.morningbrew.com/daily/stories/2022/06/14/metaverse-has-a-harassment-problem [https://perma.cc/PU6H-98JB].

127. Frenkel & Browning, *supra* note 125.

To no one's surprise, cyber gender abuse has appeared in the metaverse. Chanelle Siggens, a metaverse user, described being confronted by a male avatar who simulated ejaculating onto her avatar.[128] After she asked the player to stop, "[h]e shrugged as if to say . . . 'It's the metaverse—I'll do what I want.'"[129] Nina Jane Patel wrote about her experience being sexually harassed in VR.[130] Within a minute of her logging onto Meta's Horizon Venues, Patel's feminine-presenting avatar was surrounded by several male-presenting and male-sounding avatars who began groping and touching her avatar's body while taking selfies.[131] Patel asked the men to stop and "tried to move away, but they followed her, continuing their verbal assault and sexual advances."[132] The male avatars were "laughing, . . . aggressive, [and] . . . relentless."[133] As she removed her Oculus Quest 2 headset, she heard the men saying "'don't pretend you didn't love it,' [and] 'this is why you came here.'"[134] Because she "had a sense of presence within the [VR] room," she explained, when "[her] avatar [was attacked], [she] was attacked."[135] "It was a nightmare," Patel remarked.[136]

Thus far, Meta is following the nonrecognition playbook in refusing to address sexual harassment on its VR platforms in a meaningful manner.[137] Much

---

128. *Id.*

129. *Id.*

130. Nina Jane Patel, *Reality or Fiction?*, MEDIUM (Dec. 21, 2021), https://medium.com/kabuni/fiction-vs-non-fiction-98aa0098f3b0 [https://perma.cc/A5W5-A3JG]. Nina Jane Patel's doctoral studies focus on the psychological and physiological impact of virtual environments. Singh, *supra* note 124. She designed her avatar to look like her. Singh, *supra* note 124.

131. Singh, *supra* note 124.

132. *Id.*

133. *Id.*

134. *Id.*

135. *Id.*

136. *Id.*

137. *Cf.* Tanya Basu, *The Metaverse Has a Groping Problem Already*, MIT TECH. REV. (Dec. 16, 2021), https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem [https://perma.cc/S2AX-3BJH] (describing Meta's response to a VR sexual-harassment incident, which cited the victim's nonuse of the platform's safety tools); Joshua Zitser, *A Woman Claimed She Was Virtually Groped by a Gang of Male Avatars in Meta's Metaverse, Report Says*, BUS. INSIDER (JAN. 30, 2022, 8:50 AM EST), https://www.businessinsider.com/meta-woman-claims-virtually-groped-metaverse-horizon-venues-2022-1 [https://perma.cc/EN5L-TYHU] (same). In December 2021, a group of investors proposed that Meta "commission a third-party assessment of 'potential psychological and civil and human rights harms to users that may be caused by the use and abuse of the platform, and whether harms can be mitigated or avoided, or are unavoidable risks inherent in the technology.'" *Press Release*, *Meta Platforms (Facebook) Needs Third-Party Assessment of Metaverse User Risks and Advisory Shareholder Vote*, ARJUNA CAP. (Dec. 13, 2021), https://arjuna-

like law enforcement's response to cyberstalking and intimate-privacy violations, Meta has told female players they are responsible for virtual sexual assaults. For instance, a beta tester for Horizon Worlds "filed a complaint stating that her 'avatar had been groped by a stranger.'"[138] Meta did not take any action against the aggressor and instead "blamed the beta tester" for failing to use the platform's "personal safety features."[139]

Akin to law enforcement's refusal to address cyber abuse because it is inevitable (e.g., the "all nudes leak" observation), Meta's president for global affairs, Nick Clegg, has explained that while the company will adopt "formal rules and built-in functions" to try to curtail abuse, people inevitably "shout and swear and do all kinds of unpleasant things that aren't prohibited by law, and they harass and attack people in ways that are. The metaverse will be no different. People who want to misuse technologies will always find ways to do it."[140] Meta has introduced a "'personal boundary' feature" that prevents other players from touching a user's avatar, but given that this feature would not prevent verbal abuse, "just how much of a difference . . . this will make is not clear."[141] Beyond this, Meta is not doing much to protect players from virtual sexual assault or to respond to complaints: the Center for Countering Digital Hate "identified [and reported] 100 potential violations of platform policies" within half a day, "including sexual harassment and assault, on Meta's VRChat" — every single report went unanswered.[142]

Meta does not appear to be changing course in a more proactive direction. The company has not hired a sufficient number of content moderators for its VR

capital.com/archive/2021/12/13/press-release-meta-platforms-facebook-needs-third-party-assessment-of-metaverse-user-risks-and-advisory-shareholder-vote [https://perma.cc/T7DJ-2R4N]. During Meta's May 2022 shareholder meeting, the proposal was voted down. Weilun Soon, *A Researcher's Avatar Was Sexually Assaulted on a Metaverse Platform Owned by Meta, Making Her the Latest Victim of Sexual Abuse on Meta's Platforms, Watchdog Says*, BUS. INSIDER (May 30, 2022, 1:49 AM EST), https://www.businessinsider.com/researcher-claims-her-avatar-was-raped-on-metas-metaverse-platform-2022-5 [https://perma.cc/K7AN-4RQE]. Meta has not indicated that it will respond to those concerns of its own accord.

138. *Metaverse: Another Cesspool of Toxic Content*, SUM OF US 6 (May 2022), https://www.eko.org/images/Metaverse_report_May_2022.pdf [https://perma.cc/6ES7-WKSB].

139. *Id.*

140. Nick Clegg, *Making the Metaverse: What It Is, How It Will Be Built, and Why It Matters*, MEDIUM (May 18, 2022), https://nickclegg.medium.com/making-the-metaverse-what-it-is-how-it-will-be-built-and-why-it-matters-3710f7570b04 [https://perma.cc/69U9-L744].

141. Olivia Petter, *Why Is No One Taking Sexual Assault in the Metaverse Seriously?*, BRIT. VOGUE (Mar. 20, 2022), https://www.vogue.co.uk/arts-and-lifestyle/article/sexual-assault-in-the-metaverse [https://perma.cc/DMV3-HUUG].

142. Sophia Cho, *Sexual Assault in Immersive Virtual Reality: Criminal Law Must Keep Up with Technology*, HARV. UNDERGRADUATE L. REV. (Spring 2022), https://hulr.org/spring-2022/sexual-assault-in-immersive-vr [https://perma.cc/46H3-PJM9].

platforms, for one.[143] Andrew Bosworth, Meta's Chief Tech Officer, has said that "moderation in the metaverse 'at any meaningful scale is practically impossible.'"[144] Clegg rejected the notion that the company should be monitoring VR spaces, likening the company to a bar owner who should not "stand over your table, listen intently to your conversation, and silence you if they hear things they don't like."[145]

Meta's own experiences belie the notion that moderation is impossible. Meta employs thousands of content moderators to deal with content that violates Facebook's terms of service, including nonconsensual intimate imagery, cyberstalking, and threats.[146] Content moderators could penalize or deplatform players who repeatedly violate policies against sexual harassment and other cyber gender abuse. As Part III discusses, federal law provides an incentive for such self-monitoring by immunizing online service providers from civil liability for taking down "offensive" content, so long as they do so in good faith.[147]

In failing to address cyber gender abuse in VR, Meta is ignoring profound harms and contributing to the societal nonrecognition of cyber abuse and its gendered effects. When someone is sexually assaulted in virtual reality, they experience the groping and grabbing *in* their bodies, as Patel attested.[148] Victims *feel* the unwanted grabbing of their genitals and breasts.[149] Because VR assaults are literally felt in the body, they are arguably felt more viscerally than intimate-privacy violations or cyberstalking.[150]

---

143. SUM OF US, *supra* note 138, at 8.

144. *Id.*

145. Clegg, *supra* note 140; *see also* Kate Euphemia Clark & Trang Le, *Sexual Assault in the Metaverse Isn't a Glitch that Can Be Fixed*, MONASH UNIV. LENS (Oct. 13, 2022), https://lens.monash.edu/@politics-society/2022/10/13/1385033/sexual-assault-in-the-metaverse-isnt-a-glitch-that-can-be-fixed [https://perma.cc/QDW7-TZHV] (recognizing the inadequacy of traditional moderation tools for addressing the problem of sexual assault in the metaverse).

146. CITRON, *supra* note 22, at 172-73 (explaining that when people started using Facebook Live to livestream rapes, Mark Zuckerberg's response was to hire 3,000 more content moderators to deal with the problem).

147. 47 U.S.C. § 230(c)(2) (2018).

148. Patel, *supra* note 130.

149. Mary Anne Franks, *The Desert of the Unreal: Inequality in Virtual and Augmented Reality*, 51 U.C. DAVIS L. REV. 499, 526-28 (2017). To be sure, the harm of sexual assaults in VR differs from cyberstalking or intimate-privacy violations. Unlike cyber abuse posted online or in group texts, which can be viewed by online audiences with no ending point in sight, sexual assaults in VR have an ending point. Technically, the assaults can be stopped when attackers stop groping or, if they refuse, when victims remove their headsets. VR environments do not preserve records of avatars' activities; and search results do not index the attacks.

150. To be clear, cyberstalking and intimate-privacy violations are experienced in the body. Seeing cyberstalking when googling one's name is like a "punch in the gut," as so many victims have

Just as law enforcement's nonrecognition of cyber gender abuse sends troubling messages to victims and perpetrators, so, too, does the corporate refusal to address cyber gender abuse in virtual reality. Without a doubt, Meta's nonresponse differs from the encouragement of nonconsensual-intimate-imagery sites. But even though Meta is not soliciting sexual harassment, it is not engaging in actions that say, knock it off. Victims cannot help but understand the nonresponse as a dismissal.

C. Legal Invisibility

Unlike offline publishers and other real-space businesses that bear legal responsibility for enabling illegality, online service providers are shielded from liability for facilitating or soliciting cyber gender abuse. A federal law passed more than twenty-five years ago has been interpreted to negate any remedy brought against tech platforms for user-generated content.[151] That law, Section 230 of the Communications Decency Act, has had enormous societal consequences.[152]

At the dawn of the commercial internet, federal lawmakers recognized that government agencies could not singlehandedly address all online mischief on the horizon.[153] Representatives Chris Cox and Ron Wyden had a plan that would enable online service providers to provide "'Good Samaritan' blocking and

shared with me. When investigative journalist Rana Ayyub saw the deepfake sex video of herself, she threw up. CITRON, *supra* note 22, at 56.

151. Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, 86 FORDHAM L. REV. 401, 406-14 (2017) (discussing the overbroad interpretation of Section 230 by the state and lower federal courts).

152. For my most recent writing on Section 230, see Danielle Keats Citron, *How to Fix Section 230*, 103 B.U. L. Rev 713 (2023). Jeff Kosseff wrote a masterful book about Section 230's history, interpretation, and significance. *SEE* JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019). In *Gonzalez v. Google LLC*, 598 U.S. 617 (2023), the Supreme Court was poised to address the issue of whether a platform's algorithmic amplification of user-generated content fell within Section 230's legal shield, but the Court dodged the issue in finding that the immunity issue did not need to be resolved to resolve the cert petition. *Gonzalez*, 598 U.S. at 622. Except for Justice Jackson, all the other Justices at oral argument demonstrated an appalling lack of understanding of the history, purpose, and text of Section 230. *See* Amicus, *SCOTUS on the Internet: "It's Complicated,"* SLATE (Feb. 25, 2023, 5:00 AM), https://slate.com/podcasts/amicus/2023/02/twitter-and-google-at-the-supreme-court-left-most-of-the-justices-scratching-their-heads [https://perma.cc/S8GJ-WUKY]. As I told the *Washington Post*, I was grateful that the Supreme Court declined to rule on the breadth of Section 230(c)(1), lest they make a mess of it. Bina Venkataraman, *The Supreme Court Is Right About Google and Twitter. Now Congress Must Act*, WASH. POST (May 19, 2023, 9:21 AM) https://www.washingtonpost.com/opinions/2023/05/19/section-230-supreme-court-congress-internet-google-twitter [https://perma.cc/2EJA-KJMX].

153. Citron & Wittes, *supra* note 151, at 403.

screening of offensive material."[154] The incentive that they crafted worked in two ways. The first, Section 230(c)(1), provided online service providers with immunity from publisher or speaker liability if they left up user-generated content.[155] Section 230(c)(1) states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[156] The second, Section 230(c)(2), provided online service providers with immunity for "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."[157] The immunity of Section 230(c)(2) applies when online service providers filter, block, or take down content and when they ban, deplatform, or otherwise kick users off their services, so long as they do so voluntarily and in good faith. Section 230(c)'s legal shield has a few exemptions, including federal criminal law, intellectual property claims, and the knowing facilitation of sex trafficking.[158]

Courts *could have* strictly interpreted Section 230(c)(1) to only shield platforms from liability for claims related to the publication of another's speech, as is true for defamation and defamation-adjacent claims.[159] Courts *could have* carefully interrogated whether the gravamen of the claim for which immunity was sought was the publication of another's speech.[160] Instead, lower federal courts and state courts have broadly interpreted Section 230(c)(1) to immunize platforms from any and all claims with some relationship to user-generated material,

---

154. 47 U.S.C. § 230(c) (2018) is titled "Protection for 'Good Samaritan' Blocking and Screening of Offensive Material."

155. The subtitle of Section 230(c)(1) is "Treatment of Publisher or Speaker." 47 U.S.C. § 230(c)(1) (2018).

156. *Id.*

157. Under the subtitle "Civil Liability," Section 230(c)(2) states that providers or users of interactive computer services will not be held liable for "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected." 47 U.S.C. § 230(c)(2) (2018).

158. 47 U.S.C. § 230(e) (2018).

159. Citron, *Cyber Civil Rights*, *supra* note 25, at 116-17; Brief for Cyber Civil Rights Initiative and Legal Scholars as Amici Curiae Supporting Petitioners at 4, Gonzalez v. Google, 598 U.S. 617 (2023) (No. 21-1333) [hereinafter Brief for Cyber Civil Rights Initiative] (arguing that Section 230(c)(1) should have been interpreted to only apply to defamation and defamation-like claims).

160. Brief for Cyber Civil Rights Initiative, *supra* note 159, at 4-5.

even if those claims truly centered on the platform's own tortious actions, like a decision not to allow the blocking of IP addresses.[161]

Courts have attributed this broad-sweeping approach to the fact that "First Amendment values" drove Section 230's adoption.[162] But far more than free expression animated the adoption of Section 230. In the "Findings" and "Policy" sections of the statute, Congress articulates several goals, including to ensure that the Internet "offer[s] a forum for a true diversity of political discourse . . . and myriad avenues for intellectual activity," "to preserve the vibrant and competitive free market that presently exists for the Internet," "to encourage the development of technologies which maximize user control over what information is received," and "to ensure the vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of the computer."[163] Mary Anne Franks put it well: "[T]the law [was] intended to promote and protect the values of privacy, security and liberty alongside the values of open discourse."[164]

Under the broad judicial interpretation of Section 230(c)(1), the law has nothing to say about the enablers of harmful cyber abuse — the invisibility of law is breathtaking. The statute's legal shield has been extended to sites that intentionally solicit cyber abuse.[165] Courts have ruled that Section 230 immunizes sites like TheDirty.com that curate and post "scoops" about people, including nude images,[166] and sites devoted to intimate-privacy violations like Texxxan.com.[167] Courts have extended Section 230's legal shield to "[s]ites that

---

161. *See* Herrick v. Grindr, LLC, 306 F. Supp. 3d 579, 585-87 (S.D.N.Y. 2018), *aff'd*, 765 F. App'x 586 (2d Cir. 2019); Chi. Laws. Comm. for C.R. Under L., Inc. v. Craigslist, Inc., 519 F.3d 666, 671 (7th Cir. 2008); Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12, 29 (1st Cir. 2016); GoDaddy.com, LLC v. Toups, 429 S.W.3d 752, 759-61 (Tex. Ct. App. 2014). There have been some departures from this broad interpretation of Section 230, a gratifying though rare development. *See, e.g.*, A.M. v. Omegle.com, LLC, No. 21-cv-01674, 2022 WL 2713721, at *5 (D. Or. July 13, 2022); Lemmon v. Snap, Inc., 995 F.3d 1085, 1094 (9th Cir. 2021); Henderson v. Source for Pub. Data, L.P., 53 F.4th 110, 127-29 (4th Cir. 2022) (finding that Section 230 did not bar the claim because the online background-check service made a material contribution to the content).

162. *Doe No. 1*, 817 F.3d at 29.

163. 47 U.S.C. §§ 230(a)-(b) (2018).

164. Mary Anne Franks, *The Lawless Internet? Myths and Misconceptions About CDA Section 230*, HUFFINGTON POST (FEB. 17, 2014), https://www.huffpost.com/entry/section-230-the-lawless-internet_b_4455090 [https://perma.cc/9REU-DWJ5].

165. Citron, *supra* note 152, at 717-18.

166. *See* Jones v. Dirty World Ent. Recordings LLC, 755 F.3d 398, 402-03 (6th Cir. 2014).

167. *See* GoDaddy.com, LLC v. Toups, 429 S.W.3d 752, 753 (Tex. App. 2014); Joe Mullin, *"Revenge Porn" Victims Barred from Suing Go Daddy*, ARSTECHNICA (Apr. 14, 2014), https://arstechnica.com/tech-policy/2014/04/revenge-porn-victims-barred-from-suing-go-daddy [https://perma.cc/3V63-FZU5].

deliberately enhanced the visibility of illegality while ensuring that perpetrators could not be identified."[168] Section 230(c)(1) has been applied to negate easily administrable remedies that would have improved victims' lives immensely.[169] For instance, California's highest court has ruled that Section 230 excused Yelp from complying with a court order to remove defamatory content posted by a user.[170] Even in cases where a court has issued injunctive relief for a poster's content deemed to amount to tortious public disclosure of private fact, defamation, or intentional infliction of emotional distress, content platforms can ignore those orders because Section 230 is interpreted to shield them from having to comply.

Under the judiciary's broad interpretation of Section 230, content platforms bear no legal responsibility for the costs borne by cyber-abuse victims.[171] In turn, they can keep up, profit from, or encourage cyber abuse without fear of liability.[172] Even social networks that admittedly host child predation have enjoyed Section 230's legal shield.[173]

So, here is the current state of the law: the parties in the best position to minimize or prevent cyberstalking's damage—content platforms—bear no legal responsibility.[174] Not only can they ignore victims' pleas for help, but they can solicit or encourage cyber gender abuse. They can profit from victims' suffering. Due to Section 230, content platforms do not have to internalize the profound costs suffered by victims of cyber abuse.[175] Section 230 is why cyber abuse is legally invisible to platforms.

What about the individual perpetrators who post intimate images, dox victims, and threaten death and rape? Defenders of Section 230 advise victims to sue their attackers directly.[176] Yes, victims could sue their attackers for various torts, including defamation, public disclosure of private fact (in the case of

---

168. Citron, *supra* note 152, at 724.

169. *Id.* at 10 & nn.57-58 (discussing Hassell v. Bird, 420 P.3d 776, 779-82 (Cal. 2018)).

170. *Hassell*, 420 P.3d at 779.

171. *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, 1088-90 (2020) (reviewing NICK DRNASO, SABRINA (2018)); Citron & Wittes, *supra* note 151, at 406-10.

172. *See* Citron & Wittes, *supra* note 151, at 406-10.

173. *Id.* at 401-02; *see, e.g.*, M.H. & J.H. *ex rel.* C.H. v. Omegle.com, LLC, No. 21-cv-814, 2022 WL 93575, at *7 (M.D. Fla. Jan. 10, 2022).

174. *See* Citron, *supra* note 152, at 718-19; Citron & Wittes, *supra* note 151, at 404.

175. *See* Citron, *supra* note 152, at 726.

176. *Cf.* Jason Kelley, *Section 230 Is Good, Actually,* ELEC. FRONTIER FOUND. (Dec. 3, 2020), https://www.eff.org/deeplinks/2020/12/section-230-good-actually [https://perma.cc/P57U-5RAL] (arguing that "Section 230 means that if you break the law online, you should be the only one held responsible").

intimate images), and intentional infliction of emotional distress.[177] But practicalities make it impossible. Because Section 230 means that there are no deep pockets to sue, victims have difficulty convincing attorneys to represent them on a pro bono or low-cost basis.[178] It is hard enough to sue individual perpetrators with a lawyer, let alone without one.[179] Add to the expense of counsel the price of cyber forensic help to link cyber abuse to a perpetrator's IP address and computer, which is sometimes impossible.

Both law and practical reality mean that cyber gender abuse is not legally recognized as wrongful. This depressing state of affairs has taken a turn for the worse with a recent Supreme Court decision to which I now turn.

II. THE PROBLEM OF NONRECOGNITION COMPOUNDED BY THE SUPREME COURT

In March 2023, the Supreme Court asked Congress for millions of dollars to augment police protection of the Justices in light of escalating online threats and confrontation at their homes.[180] "On-going threat assessments show evolving risks that require continuous protection," explained the Court's budget request.[181] Yet a month later, at oral argument, members of the Court displayed a callous indifference to the interests of cyber-abuse victims. The Court's ruling in *Counterman v. Colorado* endorsed the legal nonrecognition of cyber gender abuse by making clear to victims that their speech matters less than that of their abusers. Prosecutors and law-enforcement officers are now even more likely to underenforce laws that proscribe cyber gender abuse.

177. CITRON, *supra* note 21, at 120–21.

178. CITRON, *supra* note 22, at 90–92 (explaining that victims of intimate-privacy violations cannot sue privacy invaders because they cannot afford the cost of litigation and cannot find pro bono or low bono counsel).

179. CITRON, *supra* note 21, at 162–66 (exploring the difficulties faced by plaintiffs in suing cyber harassers including difficulty in identifying perpetrators and in bringing suits under pseudonyms).

180. *Summary Statement Relating Appropriation Estimates to the Current Appropriation*, U.S. SUP. CT. 1.18, https://www.uscourts.gov/sites/default/files/Section%2001a%20Supreme%20Court%20Salaries%20and%20Expenses.pdf [https://perma.cc/RP83-S955]; Tierney Sneed & Devan Cole, *Supreme Court Asks Congress for More Security Money Due to Threats*, CNN (Mar. 9, 2023), https://www.cnn.com/2023/03/09/politics/supreme-court-security-budget-request/index.html [https://perma.cc/3PVM-L4VW].

181. *Summary Statement*, *supra* note 180, at 1.18.

A. Counterman v. Colorado *Oral Argument*

The *Counterman* case concerned a Denver-based singer-songwriter, Coles Whalen, who was terrorized by a stranger, Billy Raymond Counterman. Over two years, Whalen received hundreds of Facebook messages from Counterman. The messages suggested physical proximity — Counterman told Whalen that she looked stunning on certain evenings and that he saw her driving a white Jeep (a car she once owned).[182] Whalen repeatedly blocked him, but each time, he set up new accounts and resumed his messaging.[183] He wrote, "Knock, knock, five years on FB. I miss you, only a couple physical sightings." He started sending angry messages like "Fuck off permanently" and "Your (sic) not being good for human relations. Die, don't need you."[184] Whalen contacted law enforcement, who took her complaint seriously — a rarity — and brought her case to local prosecutors. Officers advised Whalen to carry a gun, which she reluctantly agreed to do.[185]

State prosecutors charged Counterman with emotional-distress cyberstalking (without threats), cyberstalking (with threats) and harassment (with threats), but dropped the counts covering threatening activity before trial. At trial, Whalen testified that she suffered panic attacks.[186] She explained that she had stopped doing live performances because she feared that Counterman would confront her.[187] She described her experience with "nightmares and sleepless nights and the canceled shows and not being able to go anywhere alone."[188] After Counterman was convicted and imprisoned, Whalen stopped playing music and moved across the country.[189]

On appeal, Counterman challenged the constitutionality of his conviction on the grounds that because he had not intended to scare Whalen, he could not be punished for a true threat, even though he had been convicted of emotional-

---

182. Allison Sherry, *One Colorado Stalking Victim Never Wanted to Become the Center of a First Amendment Case at the Supreme Court*, CPR NEWS (Apr. 18, 2023), https://www.cpr.org/2023/04/18/supreme-court-free-speech-colorado-stalking-case [https://perma.cc/3HMU-JZS2]; Evelyn Douek & Genevieve Lakier, *The Supreme Court Seems Poised to Decide an Imaginary Case*, ATL. (Apr. 26, 2023), https://www.theatlantic.com/ideas/archive/2023/04/supreme-court-social-media-stalking-case-colorado/673849 [https://perma.cc/2M73-RMUH].

183. Douek & Lakier, *supra* note 182.

184. Sherry, *supra* note 182; Douek & Lakier, *supra* note 182.

185. Sherry, *supra* note 182.

186. Douek & Lakier, *supra* note 182.

187. Sherry, *supra* note 182.

188. *Id.*

189. *Id.*

distress stalking and not stalking or harassment involving threats.[190] The Colorado appellate courts accepted this framing as did the Supreme Court, which granted certiorari to answer the question of whether the First Amendment requires proof that a defendant subjectively intended to terrify the victim in order to proscribe a true threat.[191]

At oral argument, little attention was paid to the destructive nature of cyberstalking. Worse, some members of the Court trivialized it. When questioning the Colorado Attorney General (AG) Phil Weiser, Chief Justice John Roberts took Counterman's texts in isolation and made light of them. Of the text "Staying in cyber life is going to kill you. Come out for coffee. You have my number," Chief Justice Roberts remarked, "I can't promise I haven't said that."[192] Laughter ensued.[193] Chief Justice Roberts suggested that the texts "might sound solicitous of the person's development."[194] Minutes before, AG Weiser underscored that ninety percent of "actual or attempted domestic violence murder cases begin with stalking."[195]

AG Weiser then explained that the text could not be interpreted without the full context—that it was a part of a tsunami of unwanted messages sent by Counterman. The Chief Justice responded by taking another text out of context—an image of a liquor bottle with the caption, "A guy's version of edible arrangements."[196] The Chief Justice's invocation of the second text elicited more laughter. Chief Justice Roberts then asked AG Weiser to "say" that text "in a threatening way," seemingly making a game out of the questioning.[197] After laughter ensued, Chief Justice Roberts repeated his request to "say that in a threatening way."[198]

Justice Gorsuch reinforced law's nonrecognition of cyber abuse by suggesting that victims might be overreacting. He said to AG Weiser, the former dean of the University of Colorado law school:

> We live in a world in which people are sensitive and—and maybe increasingly sensitive. As a professor, you might have issued a trigger warning

---

190. Douek & Lakier, *supra* note 182.

191. Douek & Lakier, *supra* note 182.

192. Transcript of Oral Argument at 53, Counterman v. Colorado, 600 U.S. 66 (2023) (No. 22-138).

193. *Id.* at 53-54.

194. *Id.* at 54.

195. *Id.* at 54.

196. *Id.* at 54.

197. *Id.* at 54-55.

198. *Id.* at 55.

> from time to time when you discuss a bit of history that is difficult or a case that's difficult. What do we do in a world in which reasonable people may deem things harmful, hurtful, threatening? And we're going to hold people liable willy-nilly for that? . . . . What do we—how do we talk about history?[199]

Justice Gorsuch's remarks suggested that cyberstalking convictions are based on "willy-nilly" guesswork and that people reporting abuse are "increasingly sensitive." It reinforced Chief Justice Roberts' dismissal of Counterman's text—"Staying in cyberlife will kill you. Come for coffee"—as an innocuous offer of help.

The Justices' refusal to recognize cyber abuse as harmful is hard to reconcile with their personal reaction to the online threats that they faced. Neither Chief Justice Roberts nor Justice Gorsuch seemingly thought that *their* request for round-the-clock police protection in the face of online threats was an overreaction. The message was clear: protection for me but not for thee.

B. Ruling and Fallout

In a 7-2 decision, the Supreme Court ruled that the First Amendment requires a heightened mental state of recklessness as to the terrorizing nature of a statement before regulating unprotected true threats.[200] The majority, written by Justice Elena Kagan, explained that, under the chilling-effects doctrine, the Court has imposed heightened *mens rea* requirements to provide "strategic protection" against the chilling of valuable speech.[201] The majority held that while threats have long been understood to fall outside the bounds of the First Amendment, proof of recklessness was necessary to protect against the "hazard of self-censorship."[202] The Court reasoned that without such a requirement, the ordinary citizen might "swallow words that are not true threats" to avoid the risk of coming near the line of illegality or getting caught up in the legal system and incurring related costs.[203] The Court justified its ruling as striking a balance in

199. *Id.* at 65.

200. *Counterman v. Colorado*, 600 U.S. 66, 73, 79-80 (2023).

201. *Id.* at 75.

202. *Id.* at 75, 77; *see also* Danielle Keats Citron, *From Bad to Worse: Threats, Stalking, and Chilling Effects*, SUP. CT. REV. (forthcoming 2024) (on file with author) (arguing that the Court made two crucial missteps in its chilling-effects analysis, leading to a one-size-fits-all model that overprotects speech with low value and that failed to accommodate the value of cyberstalking law's effort to protect victims' expression freedom).

203. *Id.* at 78.

that it was "neither the most speech-protective nor the most sensitive to the dangers of true threats."[204]

The *Counterman* ruling exacerbated the legal nonrecognition of cyber gender abuse in what it said and did.[205] How the Court talks about the values at stake conveys what it thinks is important (and what is not).[206] The majority made clear that the speech that mattered was that of people who might self-censor for fear that their words would be construed as a threat. The Court said *nothing* about the speech interests of victims. The Court acknowledged that its chilling-effects line of cases requires recognizing and "accommodating 'competing value[]' in regulating historically unprotected expression" like true threats.[207] And yet beyond noting that threats inflict "profound harms," the Court did not discuss, let alone consider accommodating, how cyberstalking and threat laws protect victims from the fear that stops them from speaking.[208] Indeed, the Court spent little time explaining why true threats do not enjoy First Amendment protection in the first place. True threats fall outside the First Amendment because they make minimal contributions to public debate and because they inflict grave harm.[209] As Professor Kenneth L. Karst has explained, legal limits on the liberty to threaten another person defend the victim's liberty to freely move around and express themselves.[210] While the majority expressed grave concern about potential abusers' self-censorship, it did not consider in its chilling-effects analysis the fact that threats coerce victims' silence.

The majority opinion exacerbates the legal nonrecognition for cyber gender abuse. The recklessness requirement could be understood as applying to all cyberstalking cases, including where abusers repeatedly violate victims' intimate privacy. Investigators might wave away victims because no threats were made, even though the stalking could be regulated consistent with the First Amendment.[211] The Court's failure to address this conundrum shows how little it thinks about the suffering of cyberstalking victims.

---

204. *Id.* at 82.

205. Citron, *Law's Expressive Value*, *supra* note 25.

206. CITRON, supra note 22, at 208-12 (emphasizing that law serves as a mirror into our values).

207. *Id.* at 80.

208. *Id.*

209. CITRON, *supra* note 21, at 202 (explaining that true threats fall outside the First Amendment because they fundamentally alter victims' lives by forcing them to leave their homes, change their activities, and retreat into silence).

210. Kenneth L. Karst, *Threats and Meanings: How the Facts Govern First Amendment Doctrine*, 58 STAN. L. REV. 1337, 1379-80 (2006).

211. Criminal laws banning nonconsensual disclosure of intimate images have faced constitutional challenges and withstood strict-scrutiny review. Citron, *supra* note 22, at 145.

The heightened mens rea requirement gives law enforcement further reason to dismiss reports of cyber gender abuse as acceptable behavior. Officers may tell victims that their hands are tied because defendants may have made a mistake and not realized that victims would be frightened.[212] Even if law enforcement investigates cases and brings them to prosecutors, prosecutors will worry that defendants can convince jurors that they never realized that they might be scaring the victims. Prosecutors will not spend resources on cases that seem unlikely to yield convictions. As AG Weiser warned at oral argument, requiring subjective intent would "immunize stalkers who are untethered from reality" and "allow devious stalkers to escape accountability by insisting that they meant nothing by their harmful statements."[213] The Court's decision will also make it even more likely that victims will under-report cyber abuse. Why bother if there is a vanishingly small chance that law enforcers will help?

Victims have discussed the terrible bind that they find themselves in. A stalker has been hounding journalist Julia Ioffe online for the past five years. One of the man's terrifying messages said, "they should put your ass to sleep."[214] Ioffe contacted the police.[215] A male detective "said, essentially, 'well, if you never said no to this guy, how is he supposed to know that you don't want him contacting you?'"[216] The detective advised Ioffe to tell the man to leave her alone, but to do so in a "nice way" so she did not "make him mad."[217] After the *Counterman* decision, the stalker contacted her, and Ioffe realized that she "had to respond to him" to tell him that she found his contact threatening and frightening.[218] The man agreed to stop sending messages, but broke his promise, saying she had been "confusing."[219] Ioffe is dismayed that she is expected to engage with her stalker, so he knows that she finds his messages unwelcome. Engaging with

---

212. Mary Anne Franks, *The Supreme Court Just Legalized Stalking*, SLATE (July 6, 2023), https://slate.com/news-and-politics/2023/07/supreme-court-legalized-stalking-counterman-colorado.html [https://perma.cc/FB3V-QDSG]; Mary Anne Franks, *How Stalking Became Free Speech*: Counterman v. Colorado *and the Supreme Court's Continuing War on Women*, GEO. WASH. L. REV. ON DOCKET (July 28, 2023), https://www.gwlr.org/how-stalking-became-free-speech-counterman-v-colorado-and-the-supreme-courts-continuing-war-on-women [https://perma.cc/38GK-76V2].

213. Transcript of Oral Argument, *supra* note 192, at 50.

214. Julia Ioffe (@juliaioffe), X (Sept. 1, 2023, 12:12 PM), https://twitter.com/juliaioffe/status/1697643717438386274 [https://perma.cc/C537-7ZFT].

215. *Id.*

216. *Id.*

217. *Id.*

218. *Id.*

219. *Id.*

stalkers gives them "the wrong idea and makes them harass you even more."[220] This is precisely what has happened with her stalker.

The oral argument and majority ruling in *Counterman* have made it all the more difficult to combat cyber gender abuse. If Supreme Court Justices can laugh about a stalker's hundreds of texts (some threatening; some suggesting physical stalking; all unwanted and frightening), why would law enforcement change course and take cyber gender abuse seriously? The ruling makes it more likely that cyber gender abuse will be ignored and unrecognized. Officers can point to *Counterman* and say it is too hard to show what stalkers understood. We need reforms so that victims get help and wrongful abuse is deterred.

III. REFORMS FOR LAW AND THE BAR

Our energy should be focused on avenues that will help make cyber gender abuse visible, unacceptable, and eradicable. The civil system can and should make clear that victims have been wronged, that the law is on their side, and that they are not to blame. First, Congress needs to bring law back into the picture for content platforms. No longer should sites whose business model is cyber gender abuse enjoy immunity from liability. Congress should ensure that all content platforms act responsibly in the face of cyber gender abuse. Then, too, victims need affordable counsel. The legal profession has a moral obligation to protect against cyber gender abuse, which drives women offline and undermines their sense of belonging and citizenship. Lawyers should devote parts of their pro bono practices to representing victims of cyber gender abuse.

A. Introducing Platform Liability (At Long Last)

In 1996, then-Representatives Christopher Cox and Ron Wyden worked on a legislative solution that would incentivize companies to moderate abusive material.[221] To that end, Section 230(c)(2) wisely shields content platforms from liability for filtering, blocking, or removing harassing and otherwise abusive material.[222] The take-down provision was (and remains) good policy. It also reflects the First Amendment rights of private companies to decide what kind of speech they want to endorse or reject.[223]

---

220. *Id.*

221. Citron, supra note 22, at 86.

222. Citron, supra note 152, at 744-746 (laying out why Section 230(c)(2) is important and consistent with First Amendment doctrine and free speech values).

223. *Id.*

Congress should spend its energy revisiting Section 230(c)(1), which provides an unchecked immunity for platforms that leave up cyber gender abuse. I have been working on a draft bill to reform Section 230 with Massachusetts Congressman Jake Auchincloss. The first part of the draft carves out from the legal shield platforms in the business of cyber gender abuse.[224] Congress never meant to provide a free pass to sites whose purpose is the destructive targeting of individuals. That would belie a key purpose of the statute, which was to deter "stalking[] and harassment by means of computer."[225] Congress must carve out those platforms from Section 230(c)(1)'s legal shield in a clear and concise way. We can do that with statutory language that threats platforms as publishers or speakers if the platform knowingly solicits, encourages, or fails to remove cyber gender abuse (i.e., cyberstalking, nonconsensual intimate imagery, or digital forgeries).

To be clear, excising bad actors from the legal shield would not mean that they would be strictly liable for users' online assaults. The law, if so reformed, would simply allow victims of cyber gender abuse to have a chance to bring legally cognizable claims against sites that encourage, solicit, or leave up such abuse.[226] Plaintiffs would have to make out cognizable claims (such as negligent enablement of crime) and prove them.[227]

Setting the outer boundaries of Section 230(c)(1) is crucial, but more is needed to deter cyber abuse and minimize the harm that it causes. Congress should set a duty of care that would require content platforms to take reasonable steps to address cyberstalking, nonconsensual intimate imagery, and digital forgeries. If those steps were taken, then the platform would be shielded from liability under Section 230(c)(1). Courts would extend the immunity to content platforms that could show that they fulfilled the duty of care, even if their efforts fell short in the particular case before the court.

The draft bill proposes steps that if followed would allow the provider of an interactive computer service not to be treated as the publisher or speaker of information involving cyberstalking, nonconsensual intimate imagery, and digital forgeries:

---

224. The draft bill is partially based on proposals that I outlined in my article, *How to Fix Section 230*, supra note 152, at 750-757.

225. 47 U.S.C. § 230(b) (2018).

226. Of course, those lawsuits would have to press claims that can be squared with the First Amendment. One can imagine that sites like Hidden Camera or Mr. Deep Fakes, which traffic in intimate-privacy violations, could face tort claims for enabling crime.

227. Citron, *supra* note 152, at 752; Citron, *Mainstreaming Privacy Torts*, *supra* note 43, at 1839-41 (discussing the potential of the tort of negligent enablement of crime against sites that solicit abuse if Section 230 were not a bar).

- First, platforms must have a process to prevent, to the extent practicable, cyberstalking, intimate-privacy violations, and digital forgeries.
- Second, platforms should have a clear and accessible process to report cyberstalking, nonconsensual intimate imagery, and digital forgeries.
- Third, platforms should have a process for addressing reports of cyberstalking, nonconsensual intimate imagery, and digital forgeries.
- Fourth, platforms should have a process to remove (or otherwise make unavailable), within 24 hours, information the provider knows or has reason to know is cyberstalking, nonconsensual intimate imagery, and digital forgeries. That process should include blocking individuals responsible for such abuse.
- Fifth, platforms should have minimum logging requirements to preserve data necessary for legal proceedings related to cyberstalking, nonconsensual intimate imagery, or digital forgeries.
- Finally, platforms should remove or block content that has been adjudicated as unlawful by a court of law.

To enable the duty of care to encompass emerging protective practices, Congress should authorize an expert independent agency like the Federal Trade Commission to engage in rulemaking to recognize new ways to take reasonable steps to address destructive online abuse.[228] An expert agency would help clarify what it means to have a process to prevent the violations. It would flag practices that meet that standard as exemplars, such as hashing programs that filter or block content designated as nonconsensual intimate imagery from being reposted.[229]

Such reform would have salutary effects. Section 230 reform would say to content platforms that they must act as guardians against cyber gender abuse, rather than throwing up their hands as Meta has done regarding virtual sexual assault. It would make clear to sites devoted to nonconsensual imagery that their business model deserves no protection because intimate-privacy violations are wrong and harmful. Protecting against cyber abuse would be something that mainstream companies would do in all stages of their business activities, from the design of their services to their content moderation practices.

As content platforms operationalize duties of care and individuals learn about them, people will feel more comfortable using those sites. In 2021, Jon

---

228. *Id.*

229. *See* Citron, *supra* note 118, at 1955-58 (discussing the use of a hashing program at Facebook for tracing and removing nonconsensual intimate imagery).

Penney, Alexis Shore, and I teamed up to conduct empirical research on the potential impact of both legal and industry efforts to protect intimate privacy (with a special focus on the responsibilities of online platforms).[230] Our preliminary findings suggest that both legal protections and industry measures would engender trust in companies and the legal system such that individuals would be more inclined to express themselves online.[231] Reforming Section 230 along these lines might encourage more expression online and offline—a win for online discourse and democracy.

Perhaps the increased adoption of augmented and virtual-reality technologies might help tip the scales. If workplaces and schools integrate augmented and virtual-reality technologies into their activities, then they should expect that those tools will be exploited to harass and stalk individuals. Unlike content platforms that enjoy immunity from liability for user-generated cyberstalking and virtual sexual assault, employers and schools enjoy no legal shield. If augmented and virtual-reality technologies produce hostile work and educational environments, then employers and school administrators ignore those abuses at their legal peril. Further, perhaps the reality of lawsuits will incentivize companies to build technologies that minimize the opportunities for abuse, reducing the risk of liability and boosting marketing and sales as a result.

Online platforms should not be largely law-free zones. To the contrary, their importance to our ability to work, socialize, and express ourselves requires that they act as guardians to ensure that cyber gender abuse does not drive people, often the most vulnerable, offline and deprive them of crucial opportunities. Careful reform of Section 230 would take us in that direction, but we also need counsel to help victims, to which I now turn.

B. Pro Bono Support

Attorneys have a crucial role to play in combating cyber abuse and they are not fulfilling that role as they could and should. Victims lack access to legal representation because they cannot afford hefty counsel fees and because attorneys do not have enough incentive to take on cases on contingency or for low cost. Yet most attorneys do some form of pro bono work—it is terrific for training young lawyers and a crucial way to provide meaningful service. Pro bono work is a badge of honor; it shows that lawyers are "officers of the court" in the most meaningful way possible.

Bar associations should urge attorneys to take on cases involving cyberstalking, intimate-privacy violations, and other cyber abuse. Pro bono cases

---

230. The Knight Foundation supported our empirical research project with a $75,000 grant.

231. Citron, *supra* note 152, at 743-45.

"traditionally involve representing people of limited means or nonprofits serving the poor."[232] Victims of cyber gender abuse come from all sorts of backgrounds. They include individuals who might be understood as middle class but who have student loans and high rents. Such individuals simply cannot afford counsel without a benefactor. Most of the victims I interviewed in my work had childcare costs, student loans, or other expenses that made paying for counsel impossible. Bar associations should recognize that efforts to protect against cyber gender abuse involve a fight for civil rights and liberties and warrant pro bono status.[233] Along similar lines, law schools have established clinics to provide free legal services for students seeking assistance related to research endeavors. For instance, the BU/MIT Student Innovations Legal Clinic provides free legal counsel to students on issues related to intellectual property, information privacy, cybersecurity, finance and business regulation, and media law.[234]

There are a few practices that take on cyber-abuse cases on a pro bono and low bono basis. K&L Gates, for instance, spearheaded the Cyber Civil Rights Legal Project (CCRLP) to represent victims of intimate-privacy violations.[235] Foley Hoag has assisted CCRI in its work. Carrie Goldberg, the country's most experienced and astute lawyer in all things cyber gender abuse, runs a law firm dedicated to intimate-privacy violations and other forms of cyber gender abuse.[236] But she can only take on so many cases on a pro bono or low bono basis—she has a small firm and needs to prioritize cases that will enable her to earn a living.[237] If we reformed Section 230, then attorneys like Goldberg would have deep pockets to sue, and she could take cases on contingency. Until such reform is passed, we need to encourage bar associations to join the fight against cyber gender abuse and encourage lawyers to include cyber-gender-abuses cases in pro bono efforts.[238]

---

232. CITRON, *supra* note 22, at 134.

233. *See id.* at 134-35.

234. *BU/MIT Student Innovations Law Clinic*, B.U. SCH. L., https://www.bu.edu/law/experiential-learning/clinics/bu-mit-student-innovations-law-clinic [https://perma.cc/49RD-5G9Y]. Professor Andrew Sellars has been leading the law school's LawTech clinic for years. He and the clinic represented Joy Buolamwini in her study of facial recognition technology called Gender Shades. *BU Law Faculty and Students Take on Algorithmic Bias*, REC., https://www.bu.edu/law/record/articles/2019/bu-law-faculty-and-students-take-on-algorithmic-bias [https://perma.cc/7A74-TYUU]. They made sure her research did not run afoul of the Computer Fraud and Abuse Act and notified companies about her research to give those companies a chance to respond and to address their products' shortcomings.

235. CITRON, *supra* note 22, at 134.

236. *Id.*

237. *Id.*

238. *Id.*

With lawyers on their side, victims would no longer feel invisible. They would hear from counsel that their suffering is real, that the "wrongs that they faced and the harms that they endured matter—that *they* matter—in the eyes of the law and society."[239] CCRI Founder Dr. Holly Jacobs told Franks and I, when we founded CCRI in 2013, that it meant the world to her that we were on her side, and that we saw her suffering in the wake of the posting of her nude images online; she felt invisible before we started working together.[240]

Legal representation and the possibility of favorable judgments matter to victims. The co-head of CCRLP, Elisa D'Amico, represented victims of intimate-privacy violations who obtained verdicts against their perpetrators.[241] D'Amico's clients knew that they would not recover much from those judgments since the perpetrators had limited funds, but the verdicts were nonetheless important to her clients.[242] D'Amico explained to me that the

> judicial rulings and awards said to her clients that what happened to them was wrong. They allowed . . . clients to see themselves as fighters with rights, rather than as naïve individuals worthy of shame, blame, or pity. No longer did her clients feel alone and helpless. They felt validated.[243]

We need the judicial system to work for victims, and having representation is an indispensable part of that effort.

CONCLUSION

By failing to recognize cyber abuse as wrongful, we have done a grave disservice to victims, their loved ones, democracy, and equality. Social recognition and legal reform are essential preconditions to meaningful course correction. Reform efforts are even more urgent given the *Counterman v. Colorado* ruling. The majority sent the message that the speech of cyberstalking victims—which we know is being silenced—is less important than the potential expression of people who might fear saying something legal lest it run afoul of stalking and threat laws. The decision made it less likely that prosecutors and law enforcement will take on cases and more likely that victims will refrain from reporting abuse.

---

239. *Id.* at 132.

240. Text Message from Holly Jacobs (June 16, 2023) (on file with author).

241. CITRON, *supra* note 22, at 132–33.

242. *Id.*

243. *Id.*

We must act now. The future will bring other forms of cyber gender abuse at a bewildering pace. When I first began writing about cyber gender abuse, perpetrators doctored people's photographs to make them appear naked and posted them online. Because the technology was crude, fakes were easily detected. Times have changed. AI programs now enable:

> anyone to turn a photo of a clothed woman into an altered version where she is naked. I'm using the pronoun "she" deliberately, because the program only works to turn photographs of people into photos of naked women. (If you submit a photo of a man or an inanimate object, it will be transformed to include breasts and female genitalia.) The program was trained on a large database of actual women's nude photographs, so it generates fake nude photos with precision, matching skin tone and swapping in breasts and genitalia in place of clothes. The program has been commercialized—an automated chatbot now takes people's orders through an encrypted messaging app and returns photos of clothed women along with naked versions. . . . [M]ore than 100,000 people have used the chatbot, and 63% of the bot's users said that they sent in photos of girls or women they knew in real life.[244]

In the fifteen years that I have been writing about cyber gender abuse, I have seen the development of deepfake technology, which is most often used to create deepfake sex videos—hyperrealistic videos of women engaging in sex in which they have never engaged.[245] I have seen the landscape of sites devoted to nonconsensual intimate images grow from forty in 2013 to more than 9,500 in 2023.[246] We need to pay attention to these developments and adopt a reform agenda before the abuse gets so far ahead of us that lawmakers, law enforcers, and companies refuse to act.

Jefferson Scholars Foundation Schenck Distinguished Professor in Law, Caddell & Chapman Professor of Law, University of Virginia School of Law; Vice President, Cyber Civil Rights Initiative; 2019 MacArthur Fellow. *I am grateful to Brianna Yang and Lydia Laramore for inviting me to write this Essay and to the team, including Dena Shata, Sara Méndez, and Jordan Kei-Rahn, for invaluable suggestions. Thanks to research assistants Jeff Stautberg and Sam Ellis and always to my partner in advocacy Dr. Mary Anne Franks and Cyber Civil Rights Initiative founder Dr. Holly Jacobs,*

244. *Id.* at 47-48.

245. *See* Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1772-73 (2019) (discussing the creation and exploitative use of deepfake sex videos).

246. Citron, *supra* note 152, at 729.

who urged us to come together to fight for change a decade ago. It has been a thrill to work on reform efforts with Representative Jake Auchincloss and his legislative aide Joe Valente alongside Mary Anne Franks and Hany Farid.