PREPARED WRITTEN TESTIMONY AND STATEMENT FOR THE RECORD FOR

Danielle Keats Citron,
Professor of Law, Boston University School of Law

HEARING ON

"Fostering a Healthier Internet to Protect Consumers"

BEFORE THE

House Committee on Energy and Commerce

October 16, 2019

John D. Dingell Room, 2123, Rayburn House Office Building

Washington, D.C.

INTRODUCTION

Thank you for inviting me to appear before you to testify about corporate responsibility for online activity and fostering a healthy internet to protect consumers. My name is Danielle Keats Citron. I am a Professor of Law at the Boston University School of Law. In addition to my home institution, I am an Affiliate Faculty at the Berkman Klein Center at Harvard Law School, Affiliate Scholar at Stanford Law School's Center on Internet & Society, Affiliate Fellow at Yale Law School's Information Society Project, and Tech Fellow at NYU Law's Policing Project. I am also a 2019 MacArthur Fellow.

My scholarship focuses on privacy, free speech, and civil rights. I have published more than 30 articles in major law reviews and more than 25 opinion pieces for major news outlets.[1] My book *Hate Crimes in Cyberspace* tackled the phenomenon of cyber stalking and what law, companies, and society can do about it.[2] As a member of the American Law Institute, I serve as an adviser on *Restatement (Third) Torts: Defamation and Privacy* and the *Restatement (Third) Information Privacy Principles Project*. In my own writing and with coauthors Benjamin Wittes, Robert Chesney, Quinta Jurecic, and Mary Anne Franks, I have explored the significance of Section 230 to civil rights and civil liberties in a digital age.[3]

* * *

Summary: In the early days of the commercial internet, lawmakers recognized that federal agencies could not possibly tackle all noxious activity online. Tech companies, in their view, were essential partners to that task. An early judicial decision, however, imperiled that possibility by

1 *See, e.g.*, Danielle Keats Citron, *Why Sexual Privacy Matters for Trust*, 96 WASH U. L. REV. (forthcoming 2019); *Sexual Privacy*, 128 YALE L.J. 1870 (2019); *When Law Frees Us to Speak,* 87 FORDHAM L. REV. 2317 (2019) (with Jonathon Penney); *Four Principles for Digital Speech*, 95 WASH. U. L. REV. 1353 (2018) (with Neil Richards); *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035 (2018); *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEXAS L. REV. (2018) (with Daniel J. Solove); *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016); *Spying Inc.*, 72 WASH. & LEE L. REV. 1243 (2015); *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345 (2014) (with Mary Anne Franks); *The Scored Society*, 89 WASH. L. REV. 1 (2014) (with Frank Pasquale); *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013) (with David Gray); *Intermediaries and Hate Speech: Fostering Digital Citizenship for the Information Age*, 91 B.U. L REV. 1435 (2011) (with Helen Norton); *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441 (2011) (with Frank Pasquale); *Mainstreaming Privacy Torts*, 99 CAL. L. REV. 1805 (2010); *Government Speech 2.0*, 87 DENVER U. L. REV. 899 (2010) (with Helen Norton); *Fulfilling Government 2.0's Promise with Robust Privacy Protections*, 78 GEO. WASH. L. REV. 822 (2010); *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373 (2009); *Cyber Civil Rights*, 89 B.U. L. REV. 61 (2009); *Technological Due Process*, 85 WASH. U. L REV. 1249 (2008); *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241 (2007).

2 DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014)

3 *See, e.g.*, Danielle Keats Citron, *Cyber Mobs, Disinformation, and Death Videos: The Internet As It Is (and as It Should Be)*, MICH. L. REV. (forthcoming 2020) (reviewing NICK DRNASO, SABRINA (2018)); *The Internet as a Speech-Conversion Machine and Other Myths Confounding Tech Policy Reform*, U. CHI. LEGAL FORUM (forthcoming 2020) (with Mary Anne Franks); *Deep Fakes: The Looming Crisis for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. (forthcoming 2019) (with Robert Chesney); *Section 230's Challenge to Civil Rights and Civil Liberties,* KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY (Apr. 6, 2008), https://knightcolumbia.org/content/section-230s-challenge-civil-rights-and-civil-liberties; *Platform Justice: Content Moderation at an Inflection Point*, HOOVER INST. (2018) (with Quinta Jurecic); *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, 86 FORDHAM L. REV. 401 (2017) (with Benjamin Wittes); *Cyber Civil Rights*, 89 B.U. L. REV. 61 (2009).

ruling that platforms' content-moderation efforts increased the risk of liability.[4] Lawmakers were appalled that online services would be penalized for self-regulation. Section 230 of the Communications Decency Act was a direct repudiation of that ruling. Congress wanted to incentivize private efforts to filter, block, or otherwise address troubling online activity.[5] Section 230 provided that incentive by securing a shield from legal liability for under- or over-filtering "offensive" content.[6]

Section 230 has helped secure opportunities to work, speak, and engage online. But it has not been a clear win for civil rights and civil liberties. Its overbroad interpretation in the courts has undermined the statute's purpose and exacted significant costs to free speech and equal opportunity. Platforms not only have been shielded from liability when their moderation efforts have filtered or blocked too much or too little "offensive" or illegal activity, as lawmakers intended. But they also have been shielded from responsibility even then they solicit illegal activities, deliberately leave up unambiguously illegal content that causes harm, and sell dangerous products. The costs to free expression and equality have been considerable, especially for women, nonwhites, and LGBTQ individuals. Section 230 should be revised to condition the legal shield on reasonable content moderation practices in the face of clear illegality that causes demonstrable harm. That would return the statute to its original purpose—to allow companies to act more responsibly, not less.

* * *

I. *Section 230's History and Purpose*

The Communications Decency Act (CDA), part of the Telecommunications Act of 1996, was introduced to make the internet safer for kids and to address concerns about pornography. Besides proposing criminal penalties for the distribution of sexually explicit material online, members of Congress underscored the need for private sector help in reducing the volume of "offensive" material online. Then-Representatives Christopher Cox and Ron Wyden offered an amendment to the CDA entitled "Protection for Private Blocking and Screening of Offensive Material."[7] The Cox-Wyden Amendment, codified as Section 230, provided immunity from liability for "Good Samaritan" online service providers that over- or under-filtered objectionable content.[8]

Section 230(c), entitled "Good Samaritan blocking and filtering of offensive content," has two key provisions. Section 230(c)(1) specifies that providers or users of interactive computer services will not be treated as publishers or speakers of user-generated content.[9] Section 230(c)(2) says that online service providers will not be held liable for good-faith filtering or blocking of user-

[4] *See* Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). For a superb history of Section 230 and the cases leading to its passage, see JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019).

[5] CITRON, HATE CRIMES IN CYBERSPACE, *supra* note, at 170-73.

[6] Citron & Wittes, *supra* note, at 404-06.

[7] *Id.*

[8] *Id.*

[9] 47 U.S.C. § 230(c)(1).

generated content.[10] Section 230 carves out exceptions from its immunity provisions, including federal criminal law, intellectual property law, and the Electronic Privacy Communications Act.[11]

In 1996, lawmakers could hardly have imagined the role that the internet would play in modern life. Yet Section 230's authors were prescient. In their view, "if this amazing new thing – the Internet – [was] going to blossom," companies should not be "punished for *trying* to keep things clean."[12] Cox recently explained that, "the original purpose of [Section 230] was to help clean up the Internet, not to facilitate people doing bad things on the Internet."[13] The key to Section 230, Wyden agreed, was "making sure that companies in return for that protection – that they wouldn't be sued indiscriminately – were being responsible in terms of policing their platforms."[14]

II. *Overbroad Judicial Interpretation*

The judiciary's interpretation of Section 230 has not squared with this vision. Rather than an immunity for responsible moderation efforts, courts have stretched Section 230's legal shield far beyond what its words, context, and purpose support.[15] Section 230 has been read to immunize platforms from liability even though they knew about users' illegal activity, deliberately refused to remove it, and ensured that those responsible for the illegality could not be identified.[16] It has provided a legal shield from liability to platforms that solicited users to engage in tortious and illegal activity.[17] It has been read to absolve platforms of liability even though they designed their sites to enhance the visibility of illegal activity and to ensure that the perpetrators could not be identified and caught.[18]

Courts have attributed this broad-sweeping approach to the fact that "First Amendment values [drove] the CDA."[19] For support, court have pointed to Section 230's "findings" and "policy" sections, which highlight the importance of the "vibrant and competitive free market that presently exists" for the internet and the internet's role in facilitating "myriad avenues for intellectual activity" and the "diversity of political discourse."[20] As Mary Anne Franks has underscored, Congress' stated goals also included the:

> development of technologies that "maximize user control over what information is received" by Internet users, as well as the "vigorous enforcement of Federal criminal laws to deter and publish trafficking in obscenity, stalking and harassment by means of the computer." In other

[10] 47 U.S.C. § 230(c)(2).
[11] 47 U.S.C. § 230(e).
[12] See Citron & Jurecic, *supra* note.
[13] *Id.*
[14] *Id.*
[15] Citron & Wittes, *supra* note, at 406-10.
[16] *Id.*
[17] *Id.*
[18] Citron, *Section 230's Challenge to Civil Rights and Civil Liberties*, *supra* note. *See generally* Olivier Sylvain, *Intermediary Design Duties*, 50 CONN. L. REV. 1 (2017).
[19] Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12, 18 (1st Cir. 2016), cert. denied, 137 S. Ct. 622 (2017).
[20] See, e.g., Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009).

words, the law [wa]s intended to promote the values of privacy, security and liberty alongside the values of open discourse.[21]

Section 230's liability shield has been extended to shield activity that has little to do with free speech, including the sale of dangerous products.[22] Consider Armslist.com, the self-described "firearms marketplace."[23] Unlicensed sellers use the site to sell guns to people who cannot pass background checks.[24] Armslist.com is where Radcliffe Haughton illegally purchased a gun, which he used to murder his estranged wife who had a restraining order against him.[25] The Wisconsin court's restraining order banned Haughton from legally purchasing a firearm.[26] On Armslist.com, Haughton found a gun seller that did not require a background check.[27] He used the gun that he illegally purchased to murder his estranged wife and two co-workers.[28] The Wisconsin Supreme Court held that Armslist was immune from liability based on Section 230.[29]

Extending the immunity from liability to platforms that deliberately encourage, facilitate, or refuse to remove illegal activity would seem absurd to the CDA's drafters. But even more absurd is immunizing from liability enterprises that connect sellers of deadly weapons with prohibited buyers for a cut of the profits. Armslist.com can hardly be said to "provide 'educational and informational resources' or contribute to 'the diversity of political discourse.'"[30]

III. *Evaluating the Status Quo*

Section 230's overbroad interpretation means that platforms have little legal incentive to combat online abuse. Rebecca Tushnet put it well a decade ago: Section 230 ensures that platforms enjoy "power without responsibility."[31] Market forces are unlikely to encourage responsible content moderation. Platforms make their money through online advertising generated when users like, click, and share.[32] Thus, allowing attention-grabbing abuse to remain online accords with platforms' rational self-interest. Platforms "produce nothing and sell nothing except advertisements and information about users, and conflict among those users may be good for business."[33] If a company's analytics suggest that people pay more attention to content that makes

21 Mary Anne Franks, *The Lawless Internet? Myths and Misconceptions About CDA Section 230*, HUFFINGTON POST (Feb. 17, 2014).
22 *See, e.g.*, Hinton v. Amazon.com, LLC, 72 F. Supp. 3d 685, 687, 690 (S.D. Miss. 2014).
23 https://www.armslist.com/
24 See Mary Anne Franks, *Our Collective Responsibility for Mass Shootings*, N.Y. TIMES, October 11, 2019, available at https://www.nytimes.com/2019/10/09/opinion/mass-shooting-responsibility.html.
25 *Id.*
26 *Id.*
27 *Id.*
28 *Id.*
29 *Id.* The non-profit organization the Cyber Civil Rights Initiative, of which I am the Vice President alongside Dr. Mary Anne Franks who serves as its President, has filed an amicus brief in support of the petitioner's request for writ of certiorari in the Supreme Court. Brief of Amicus Curiae of Cyber Civil Rights Initiative and Legal Academics in Support of Petitioners in Yasmine Daniel v. Armslist.com, *available at* https://www.supremecourt.gov/DocketPDF/19/19-153/114340/20190830155050530_Brief.PDF
30 Amicus Curiae of Cyber Civil Right Initiative, *supra* note 29, at 16.
31 Rebecca Tushnet, *Power without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986 (2008).
32 Mary Anne Franks, *Justice Beyond Dispute*, 131 HARV. L. REV. 1374, 1386 (2018) (reviewing ETHAN KATSH & ORNA RABINOVICH-EINY, DIGITAL JUSTICE: TECHNOLOGY AND THE INTERNET OF DISPUTES (2017)).
33 *Id.*

them sad or angry, then the company will highlight such content.[34] Research shows that people are more attracted to negative and novel information.[35] Hence, keeping up destructive content may make the most sense for a company's bottom line.

As Federal Trade Commissioner Rohit Chopra powerfully warned in his dissent from the agency's 2019 settlement with Facebook, the behavioral advertising business model is the "root cause of [social media companies'] widespread and systemic problems."[36] Online behavioral advertising generates profits by "turning users into products, their activity into assets," and their platforms into "weapons of mass manipulation."[37] Tech companies "have few incentives to stop [online abuse], and in some cases are incentivized to ignore or aggravate [it]."[38]

To be sure, the dominant tech companies do moderate certain content by shadow banning, filtering, or blocking it.[39] They have acceded to pressure from the European Commission to remove hate speech and terrorist activity.[40] They have banned certain forms of online abuse, such as nonconsensual pornography and threats, in response to pressure from users, advocacy groups, and advertisers.[41] Platforms have expended resources to stem abuse when it is a net negative for their bottom line.[42]

Yet, as we have seen, market pressures do not always point in that direction. The business model of some sites is abuse because such abuse generates online traffic, clicks, and shares.[43] Deepfake pornography sites[44] as well as countless revenge porn sites and gossip sites[45] thrive thanks to online advertising.

Without question, Section 230 has been valuable to innovation and expression. It has enabled vast and sundry businesses. It has led to the rise of social media companies like Facebook, Twitter, and Reddit. But it also has subsidized platforms that encourage online abuse. It has left victims without leverage to insist that platforms take down destructive activity.

[34] Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc*., Commission File No. 1823109, at 2 (July 24, 2019).
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] Franks, *Justice Beyond Dispute*, *supra* note, at 1386.
[39] Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, *supra* note, at 1038-39; Citron & Norton, *Intermediaries and Hate Speech*, *supra* note, at 1468-71.
[40] Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, *supra* note, at 1038-39.
[41] *Id.* at 1037.
[42] CITRON, HATE CRIMES IN CYBERSPACE, *supra* note, at 229 (discussing how Facebook changed its position on pro rape pages after fifteen companies threatened to pull their ads); Mary Anne Franks, *"Revenge Porn" Reform: A View from the Front Lines*, 69 FLA. L. REV. 1251 (2017).
[43] For instance, eight of the top ten pornography websites host deepfake pornography, and there are nine deepfake pornography websites hosting 13,254 fake porn videos (mostly featuring female celebrities without their consent). These sites generate income from advertising. Indeed, as the first comprehensive study of deepfake video and audio explains, "deepfake pornography represents a growing business opportunity, with all of these websites featuring some form of advertising." Deeptrace Labs, *The State of Deepfakes: Landscape, Threats, and Impact* 6 (September 2019), available at https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf.
[44] *Id.*
[45] *See, e.g.*, *Erna Besic Psycho Mom of Two!*, THEDIRTY (Oct. 9, 2019, 10:02 AM), https://thedirty.com/#post-2374229.

This laissez-faire approach has been costly to individuals, groups, and society. As more than ten years of research have shown, cybermobs and individual harassers target individuals with sexually threatening and sexually humiliating online abuse.[46] According to a 2017 Pew Research Center study, one in five U.S. adults have experienced online harassment that includes stalking, threats of violence, or cyber sexual harassment.[47] More often, targeted individuals are women, women of color, lesbian and trans women, and other sexual minorities.[48] They do not feel safe on- or offline.[49] They experience anxiety and severe emotional distress. Some victims move and change their names.[50]

In the face of online assaults, victims have difficulty finding employment or keeping their jobs because the abuse appears in searches of their names.[51] Online abuse not only makes it difficult to make a living, but it silences victims.[52] Targeted individuals often shut down social media profiles, blogs, and accounts.[53] As Mary Anne Franks has argued in her important new book *The Cult of the Constitution*, a strike-oriented view of Section 230 has been costly to equal protection.[54] The benefits Section 230's immunity has enabled likely could have been secured at a lesser price.[55]

IV. *Potential Statutory Responses*

Reforming Section 230 is long overdue. Before discussing possible options, it is worth noting that efforts are underway to impose Section 230's provisions as part of trade agreement with Mexico and Canada. It is unwise for the Administration to inscribe Section 230 into trade agreements at the same time that efforts are underway in Congress to reform the law.[56]

[46] *See generally* CITRON, HATE CRIMES IN CYBERSPACE, *supra* note. The 2017 Pew study found that one in four Black individuals say they have been subject to online harassment due to their race as have one in ten Hispanic individuals. For white individuals, the share is lower—three percent. Women are twice as likely as men to say they have been targeted online due to their gender (11 percent versus 5 percent). Duggan, *supra* note. Other studies have made clear that LGBTQ individuals are particularly vulnerable to online harassment, CITRON, HATE CRIMES IN CYBERSPACE, *supra* note, as well as nonconsensual pornography. Data & Society, Online Harassment, Digital Abuse, and Cyberstalking in America (November 21, 2016), *available at* https://innovativepublichealth.org/wp-content/uploads/2_Online-Harassment-Report_Final.pdf.

[47] Maeve Duggan, Online Harassment 2017 Study, Pew Research Center (July 11, 2017).

[48] CITRON, HATE CRIMES IN CYBERSPACE, *supra* note.

[49] *Id.*

[50] Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117, 125–26 (2016); *see also* Jonathon W. Penney, *Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study*, 6 INTERNET POL'Y REV., May 26, 2017, at 1, 3. *See generally* CITRON, HATE CRIMES IN CYBERSPACE, *supra* note, at; Danielle Keats Citron, *Civil Rights In Our Information Age*, in THE OFFENSIVE INTERNET (Saul Levmore & Martha C. Nussbaum, eds. 2010); Citron & Richards, *supra* note, at 1365 ("[N]ot everyone can freely engage online. This is especially true for women, minorities, and political dissenters who are more often the targets of cyber mobs and individual harassers."); Citron & Franks, *supra* note, at 385; Citron, *Cyber Civil Rights*, *supra* note.

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] MARY ANNE FRANKS, THE CULT OF THE CONSTITUTION (2019).

[55] Citron & Wittes, *supra* note.

[56] *See, e.g.*, Neil Turkewitz, *NAFTA and Unsafe Harbors: Why Calls for Blanket Immunities Must Be Rejected*, MEDIUM (Jan. 23, 2018). As Rebecca J. Hamilton explores in her important work, there is and should not be a one-size fits all model for online speech regulation given the socio-legal-cultural differences in the global public spheres online. Rebecca J. Hamilton, *Governing the Global Public Sphere* (on file with author).

Some urge Congress to maintain Section 230's immunity but to create an explicit exception from its legal shield for certain types of behavior. A recent example of that approach is the Stop Enabling Sex Traffickers Act (SESTA), which passed by an overwhelming vote in 2016. The bill amended Section 230 by rendering websites liable for knowingly hosting sex trafficking content. That law, however, is flawed. By effectively pinning the legal shield on a platform's lack of knowledge of sex trafficking, the law reprises the dilemma that led Congress to pass Section 230 in the first place. To avoid liability, platforms have resorted to either filtering everything related to sex or sitting on their hands.[57] That is the opposite of what the drafters of Section 230 wanted.

There are better alternatives. A more effective and modest adjustment would involve amending Section 230 to exclude bad actors from its legal shield. Free speech scholar Geoffrey Stone, for instance, suggests denying the immunity to online service providers that "deliberately leave up unambiguously unlawful content that clearly creates a serious harm to others."[58]

A variant on this theme would deny the legal shield to cases involving platforms that have solicited or induced illegal behavior or unlawful content. This approach takes a page from intermediary liability rules in trademark and copyright law. As Stacey Dogan observed in that context, inducement doctrines allow courts to target bad actors whose business models center on infringement.[59] Providers that solicit or induce illegality should not enjoy immunity from liability. This approach targets the harmful conduct while providing breathing space for protected expression.[60]

There is a broader, though balanced, legislative fix that Benjamin Wittes and I have proposed. Under our proposal, platforms would enjoy immunity from liability *if* they could show that their content-moderation practices writ large are reasonable. Wittes and I offer a revision to Section 230(c)(1) as follows:

> No provider or user of an interactive computer service that *takes reasonable steps to address known unlawful uses of its services that create serious harm to others* shall be treated as the publisher or speaker of any information provided by another information content provider *in any action arising out of the publication of content provided by that information content provider*.

If adopted, the question before the courts in a motion to dismiss on Section 230 grounds would be whether a defendant employed reasonable content moderation practices in the face of known illegality. The question would not be whether a platform acted reasonably with regard to a specific instance of speech. Instead, the court would ask whether the platform engaged in reasonable content moderation practices writ large with regard to known illegality that creates serious harm to others.[61]

[57] Citron & Jurecic, *supra* note.
[58] E-mail from Geoffrey Stone, Professor of Law, Univ. of Chi., to author (Apr. 8, 2018).
[59] Stacey Dogan, *Principled Standards vs. Boundless Discretion: A Tale of Two Approaches to Intermediary Trademark Liability Online*, 37 COLUM. J.L. & ARTS 503, 507-08 (2014).
[60] *Id.* at 508-09.
[61] Tech companies have signaled their support as well. For instance, IBM issued a statement saying that Congress should adopt our proposal and wrote a tweet to that effect as well. Ryan Hagemann, *A Precision Approach to Stopping Illegal Online Activities,* IBM THINK POLICY (July 10, 2019), https://www.ibm.com/blogs/policy/cda-230/; *see also*

The assessment of reasonable content-moderation practices would take into account differences among online entities. Social networks with millions of postings a day cannot plausibly respond to complaints of abuse immediately, let alone within a day or two. On the other hand, they may be able to deploy technologies to detect and filter content that they previously determined was unlawful.[62] The duty of care will evolve as technology improves.

A reasonable standard of care will reduce opportunities for abuse without interfering with the further development of a vibrant internet or unintentionally turning innocent platforms into involuntary insurers for those injured through their sites. Approaching the problem as one of setting an appropriate standard of care more readily allows differentiating between different kinds of online actors. Websites that solicit illegality or that refuse to address unlawful activity that creates serious harm should not enjoy immunity from liability. On the other hand, social networks that have safety and speech policies that are transparent and reasonably executed at scale should enjoy the immunity from liability as the drafters of Section 230 intended.

To return to Rebecca Tushnet's framing, with power comes responsibility. Law should change to ensure that such power is wielded responsibly. With Section 230, Congress sought to provide incentives for "Good Samaritans" engaged in efforts to moderate content. Their goal was laudable. Section 230 should be amended to condition the immunity on reasonable moderation practices rather than the free pass that exists today. Market pressures and morals are not always enough, and they should not have to be.

BIOGRAPHY

Danielle Citron is a Professor of Law at the Boston University School of Law. She previously taught at the University of Maryland Carey School of Law where she received the 2018 "UMD Champion of Excellence" award for teaching and scholarship. Professor Citron has been a Visiting Professor at Fordham University School of Law (Fall 2018) and George Washington Law School (Spring 2017). Professor Citron teaches and writes about data privacy, free expression, civil rights, and administrative law.

Professor Citron is an internationally recognized privacy expert. She was named a MacArthur Fellow in 2019. Her book *Hate Crimes in Cyberspace* (Harvard University Press) explored the phenomenon of cyber stalking and the role of law and private companies in combating it. The editors of *Cosmopolitan* included her book in its "20 Best Moments for Women in 2014." Professor Citron has published numerous book chapters and more than 30 law review articles, published in the *Yale Law Journal*, *California Law Review*, *Michigan Law Review*, *Harvard Law Review Forum*, *Boston University Law Review*, *Notre Dame Law Review*, *Fordham Law Review*, *George Washington Law Review*, *Minnesota Law Review*, *Texas Law Review*, *Washington University Law Review*, *Southern California Law Review*, *Washington & Lee Law Review*, *Wake Forest Law Review*, *Washington Law*

@RyanLeeHagemann, TWITTER (July 10, 2019, 3:14 PM), https://twitter.com/RyanLeeHagemann/status/1149035886945939457?s=20 ("A special shoutout to @daniellecitron and @benjaminwittes, who helped to clarify what a moderate, compromise-oriented approach to the #Section230 debate looks like.").

[62] Citron, *Sexual Privacy*, *supra* note (discussing Facebook's hashing initiative to address nonconsensual distribution of intimate images).

Review, *U.C. Davis Law Review*, *University of Chicago Legal Forum*, and other journals. Her current scholarly projects concern sexual privacy; privacy and national security challenges of deep fakes; and the automated administrative state. Professor Citron's opinion pieces have appeared in major media outlets, including *The New York Times*, *The Atlantic*, *Slate*, *Time*, *CNN*, *The Guardia*n, *New Scientist*, *Lawfare*, *ars technica*, and *New York Daily News*. She is a technology contributor for *Forbes* and served as a member of the now-defunct *Concurring Opinions* blog (2008-2019).

Professor Citron's work has been recognized at home and abroad. In 2015, the United Kingdom's *Prospect Magazine* named Professor Citron one of the "Top 50 World Thinkers." *The Maryland Daily Record* named her one of the "Top 50 Most Influential Marylanders." In 2011, Professor Citron testified about misogynistic cyber hate speech before the Inter-Parliamentary Committee on Anti-Semitism at the House of Commons.

Professor Citron is an active member of the cyber law community. She is an Affiliate Scholar at the Stanford Center on Internet and Society, Affiliate Fellow at the Yale Information Society Project, Senior Fellow at Future of Privacy, Affiliate Faculty at the Berkman Klein Center at Harvard Law School, and a Tech Fellow at the NYU Policing Project. She is a member of the American Law Institute (inducted in 2017) and serves as an adviser to the American Law Institute's *Restatement (Third) Information Privacy Principles Project* and *Restatement (Third) Torts: Defamation and Privacy*.

Professor Citron works with civil liberties and privacy organizations. She is the Vice President of the *Cyber Civil Rights Initiative*. She served as the Chair of the *Electronic Privacy Information Center*'s Board of Directors from 2017-2019 and now sits on its Board. Professor Citron has served on the Advisory Boards of *Without My Consent*, *Teach Privacy*, and the *International Association of Privacy Professionals* Privacy Bar. In connection with her advocacy work, she advises tech companies on online safety, privacy, and free speech. She serves on Twitter's Trust and Safety Council as well as Facebook's Nonconsensual Intimate Imagery Task Force. She has presented her research at Twitter, Facebook, Google, and Microsoft.

Professor Citron advises federal and state legislators, law enforcement, and international lawmakers on privacy issues. In June 2019, she testified at the House Intelligence Committee hearing on deep fakes and other forms of disinformation. In July 2017, she testified at a congressional briefing on online harassment and sexual violence co-sponsored by Congresswoman Jackie Speier. In April 2015, she testified at a congressional briefing sponsored by Congresswoman Katharine Clark on the First Amendment implications of a federal cyber stalking legal agenda. She has worked with the offices of Congresswoman Jackie Spier, Congresswoman Katharine Clark, Senator Richard Blumenthal, Senator Elizabeth Warren, Senator Kamala Harris, and Senator Diane Feinstein on federal legislation. Professor Citron helped Maryland State Senator Jon Cardin draft a bill criminalizing the nonconsensual publication of nude images, which was passed into law in 2014. From 2014 to December 2016, Professor Citron served as an advisor to then-California Attorney General Kamala Harris. She served as a member of AG Harris's *Task Force to Combat Cyber Exploitation and Violence Against Women*. In October 2015, Professor Citron, with AG Harris, spoke at a press conference to discuss the AG office's new online hub of resources for law enforcement, technology companies, and victims of cyber sexual exploitation.

Professor Citron has presented her research in over 200 talks at federal agencies, meetings of the National Association of Attorneys General, the National Holocaust Museum, the Anti-Defamation League, Wikimedia Foundation, universities, companies, and think tanks. She gave a TED talk on the issue of deep fakes at the 2019 Global TED Summit in Edinburgh, Scotland. She appeared in HBO's *Swiped: Hooking Up in the Digital Age* (directed by Nancy Jo Sales) and *Netizens* (which premiered at the 2018 Tribeca Film Festival, directed by Cynthia Lowen). She has been quoted in hundreds of news stories in publications including *The New York Times*, *Washington Post*, *Wall Street Journal*, *Los Angeles Times*, *San Francisco Chronicle*, *USA Today*, *National Public Radio*, *Time*, *Newsweek*, *the New Yorker*, *New York Magazine*, *Cosmopolitan*, HBO's Last Week Tonigh with John Oliver *Barron's*, *Financial Times*, *The Guardian*, *Vice News*, and *BBC*. She is a frequent radio guest, appearing on National Public Radio shows, including *All Things Considered*, WHYY's *Radio Times*, WNYC's *Public Radio International*, Minnesota Public Radio, WYPR's *Midday with Dan Rodricks*, Wisconsin Public Radio, WAMU's *1A*, WAMU's *The Diane Rehm Show*, and Chicago Public Radio.