Stanford | Cyber Policy Center
Freeman Spogli Institute

REFORMING SECTION 230 AND PLATFORM LIABILITY

STANFORD UNIVERSITY

Dr. Mary Anne Franks

Professor of Law and Dean's Distinguished Scholar, University of Miami School of Law
President and Legislative & Tech Policy Director, Cyber Civil Rights Initiative

REFORMING SECTION 230 AND PLATFORM LIABILITY

Insulating the tech industry from liability for online extremism, abuse, and misinformation has threatened free expression, worsened existing inequalities of gender, race, and class, and gravely undermined democracy. The tech industry can no longer be exempted from the principle of collective responsibility for harm.

THE PROBLEM

On Jan. 8, 2021, two days after a violent mob attacked the United States Capitol in an attempt to prevent Congress's certification of the 2020 presidential election, the social media platform Twitter permanently **banned** President Donald Trump's personal account. Twitter had temporarily locked the @realDonaldTrump account on Jan. 6 after Trump posted a video and a statement repeating false claims about the election and expressing his "**love**" for the rioters, requiring Trump to delete the tweets before being able to post again. At the time of the **lockout**, the Twitter Safety team noted that if Trump violated Twitter's policies again his account would be banned. In a **blog post** on Jan. 8, the company explained that it had determined that two of Trump's tweets following the riots, one referencing "American Patriots" and another stating that Trump would not be attending President-Elect Joseph R. Biden's inauguration, were "likely to inspire others to replicate the violent acts that took place on Jan. 6, 2021, and that there are multiple indicators that they are being received and understood as encouragement to do so."

The rioters who **attacked** the Capitol on Jan. 6 bludgeoned a police officer to death with a fire extinguisher; dragged another officer down several steps and beat him with an American flag; attempted to locate and assassinate Speaker of the House Nancy Pelosi; constructed a gallows on Capitol grounds and called for the hanging of Vice President Mike Pence; ransacked Congressional offices; looted federal property; and forced terrified elected

officials and their staff into hiding for several hours. The rioters **organized** their efforts on sites such as Facebook, Twitter, and Parler, where false claims about election fraud and increasingly unhinged conspiracy theories like QAnon had proliferated for months.

Twitter's decision to ban Trump came after Facebook's announcement that it would be suspending Trump's account **indefinitely**; more **social media bans** – not just of Trump, but of other individuals who promoted lies about the election, endorsed white supremacist rhetoric and violence, or encouraged further insurrection efforts - quickly followed. On Jan. 9, Google and Apple removed the rightwing-dominated social media site **Parler** from their app stores after the site refused to moderate violent content, and Amazon removed the site from its web hosting services later that same day, citing the platform's multiple violations of Amazon's terms of service.

While many praised the social media crackdown, several prominent Republican figures **characterized** it as an attack on free speech and the First Amendment – often taking to social media to do so. Secretary of State Mike Pompeo tweeted, "Silencing speech is dangerous. It's un-American. Sadly, this isn't a new tactic of the Left. They've worked to silence opposing voices for years." Trump's son, Donald Trump Jr., tweeted, "Free Speech Is Under Attack! Censorship is happening like NEVER before! Don't let them silence us." Congressman Matt Gaetz **proclaimed**, on Twitter, "We cannot live in a world where Twitter's terms of service are more important than the terms in our Constitution and Bill of Rights."

Many conservatives also complained about how many **followers they were losing** as Twitter purged accounts violating their terms of service. Pompeo tweeted a graphic purporting to show how many thousands of followers he and other high-profile right-wing individuals had lost. Scott Atlas, who served as a Trump advisor on COVID-19 policy, bemoaned on Jan.11, "I have lost 12k followers in the past few days." Sarah Huckabee Sanders, the former White House press secretary, tweeted on Jan. 9, "I've lost 50k+ followers this week. The radical left and their big tech allies cannot marginalize, censor, or silence the American people. This is not China, this is United States of America, and we are a free country."

But it was not only conservatives who raised concerns about social media platforms banning Trump and cracking down on election disinformation and violent propaganda. Following Facebook's indefinite suspension of Trump's account, National Security Agency whistleblower Edward Snowden **tweeted**, "Facebook officially silences the President of the United States. For better or worse, this will be remembered as a turning point in the battle for control over digital speech." The Electronic Frontier Foundation (EFF) somberly **observed** that "we are always concerned when platforms take on the role of censors." A senior legislative counsel for the American Civil Liberties Union (ACLU) **wrote** "it should concern everyone when companies like Facebook and Twitter wield the unchecked power to remove people from platforms that have become indispensable for the speech of billions." ACLU attorney Ben Wizner criticized Amazon's decision to cut off Parler, **telling** the New York Times that "[t]here will be times when large majorities of people want to repel speech that is genuinely important… I think we should encourage, in a broad sense, companies like Amazon to embrace neutrality principles so that there can be a diversity of voices online."

The swift social media crackdown on harmful online content following the events of Jan. 6 demonstrated that technology companies have long had the capacity to address online extremism and abuse – they have only lacked the will. And the cries of censorship that these belated and modest moves have triggered from influential figures across the political spectrum helps explain why that will has been lacking for so long. The telecommunications industry has actively encouraged the public to think of online platforms as natural, essential, and unmediated outlets for free speech. Society has become so dependent on social media for communication, news, commerce, education, and entertainment that any restriction of access feels like a violation of **constitutional significance**. The outsized influence of the internet over daily life leads users to think of online platforms and tech companies not as the premises and products of private businesses, but as public forums controlled by quasi-governmental actors.

The tech industry's invocation of "free speech" as a core value contributes greatly to the American public's confusion between state action restricting

Powerful tech companies have for decades been invoking the laissez-faire principles of the First Amendment to absolve themselves of responsibility for abuse and extremism that flourish on their platforms and services, undermining the concept of collective responsibility that is central to a functioning society, both online and off.

speech, which implicates the First Amendment, and private action, which does not. It also contributes to the erasure of the distinction between speech and conduct, and the distinction between speech protected by the First Amendment and speech that is not. Powerful tech companies have for decades been invoking the laissez-faire principles of the First Amendment to absolve themselves of responsibility for abuse and extremism that flourish on their platforms and services, undermining the concept of **collective responsibility** that is central to a functioning society, both online and off.

The most powerful tool for this destructive agenda has been Section 230 of the Communications Decency Act, which courts have interpreted as broadly insulating online intermediaries from liability even when they knowingly benefit from harmful content and conduct on their platforms and services. Courts have interpreted Section 230 to protect online classifieds sites from responsibility for advertising sex trafficking, online firearms sellers from responsibility for facilitating unlawful gun sales, online marketplaces from responsibility for putting defective products into the stream of commerce, and social media platforms from responsibility for the organization and encouragement of terrorist acts.

Section 230 has, without a doubt, produced a wealth of expressive, economic, and informational benefits. But both the benefits and the harms

flowing from the exceptional immunity granted to the tech industry are unequally distributed. For while the anti-regulatory, pro-corporation, techno-utopian system made possible by courts' expansive interpretation of Section 230 immunity generates enormous capital, both literal and symbolic, the vast majority of that capital stays firmly in the hands of those who have always had more of it than everyone else: the wealthy, the white, the male. While Section 230 does indeed amplify free speech, increase profits, and enable informational dominance for the powerful and the privileged, it also enables the silencing, bankrupting, and subordination of the vulnerable.

The concept of "cyber civil rights" (a phrase coined by Professor Danielle Keats Citron in 2009), highlights how the internet has rolled back many recent gains in racial and gender equality. The anonymity, amplification, and aggregation possibilities offered by the internet have allowed private actors to discriminate, harass, and threaten vulnerable groups on a massive,

While Section 230 does indeed amplify free speech, increase profits, and enable informational dominance for the powerful and the privileged, it also enables the silencing, bankrupting, and subordination of the vulnerable.

unprecedented scale. Abundant empirical evidence demonstrates that online abuse further chills the intimate, artistic, and professional expression of individuals whose rights were already under assault offline. As the internet has multiplied the possibilities of expression, it has also multiplied the possibilities of repression, facilitating a censorious backlash against women and minorities. The internet lowers the costs of abuse by providing abusers with anonymity and social validation, while providing new ways to increase

We are all living in the world Section 230 built: where expressive, economic, and information inequalities divide our society; where a President can use social media platforms to incite violence against his own citizens; where domestic terrorists can coordinate bloody attacks on the Capitol; where global corporations can extract astronomical profits from exploiting private data, where women and minorities are silenced by online mobs, and where massive disinformation and misinformation campaigns can micro-target populations to create public health crises, foment armed rebellions, and undermine democracy itself.

the range and impact of that abuse. The online abuse of women in particular amplifies sexist stereotyping and discrimination, compromising gender equality online and off.

We are all living in the world Section 230 built: where expressive, economic, and information inequalities divide our society; where a President can use social media platforms to incite violence against his own citizens; where domestic terrorists can coordinate bloody attacks on the Capitol; where global corporations can extract astronomical profits from exploiting private data, where women and minorities are silenced by online mobs, and where massive disinformation and misinformation campaigns can micro-target populations to create public health crises, foment armed rebellions, and undermine democracy itself.

RECOMMENDATIONS

In light of the foregoing, the Biden-Harris Administration should take the following three steps.

1. Instruct Congress to pass legislation that amends Section 230 to protect online intermediaries against liability only for the speech of third parties and to deny immunity to platforms that demonstrate deliberate indifference to harmful content.

A. Explicitly limiting Section 230's protections to speech.

Both critics and defenders of Section 230 agree that the statute provides online intermediaries broad immunity from liability for a wide range of internet activity. While critics of Section 230 point to the extensive range of harmful activity that the law's deregulatory stance effectively allows to flourish, Section 230 defenders argue that an unfettered internet is vital to a robust online marketplace of ideas. The marketplace of ideas is a familiar and powerful concept in First Amendment doctrine, serving as a justification for a laissez-faire approach to speech. Its central claim is that the best approach to bad or harmful speech is to let it circulate freely, because letting ideas compete in the market is the best way to sort truth from falsity and good speech from bad speech.

The internet-as-marketplace-of-ideas presumes, first of all, that the internet is primarily, if not exclusively, a medium of speech. The text of Section 230 reinforces this characterization through the use of the terms "publish," "publishers," "speech," and "speakers" in 230(c), as well as the finding that the "Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."

When Section 230 was passed, it may have made sense to think of the internet as a speech machine. In 1996, the internet was text-based and predominantly noncommercial. Only 20 million American adults had internet access, and these users spent less than half an hour a month online. But by 2019, 293 million Americans were using the internet, and they were using it not only to communicate, but also to buy and sell merchandise, find dates, make restaurant reservations, watch television, read books, stream music, and look for jobs. According to Section 230 **enthusiast**,

> the entire suite of products we think of as the internet—search engines, social media, online publications with comments sections, Wikis, private message boards, matchmaking apps, job search sites, consumer

> review tools, digital marketplaces, Airbnb, cloud storage companies, podcast distributors, app stores, GIF clearinghouses, crowdsourced funding platforms, chat tools, email newsletters, online classifieds, video sharing venues, and the vast majority of what makes up our day-to-day digital experience—have benefited from the protections offered by Section 230.

But many of these "products" have very little to do with speech and, indeed, many of their offline cognates would not be considered speech for First Amendment purposes. If, as many defenders of Section 230 as currently written would have it, the broad immunity afforded online intermediaries is justified on First Amendment principles, then it should apply only with regard to online activity that can plausibly be characterized as speech. What is more, it should only apply to third-party speech for which platforms serve as true intermediaries, not speech that the platform itself creates, controls, or profits from.

Section 230 should be amended to make explicitly clear that the statute's protections only apply to speech by replacing the word "information" in (c)(1) with the word "speech." This revision would put all parties in a Section 230 case on notice that the classification of content as speech is not a given, but a fact to be demonstrated. If a platform cannot make a showing that the content or information at issue is speech, then it should not be able to take advantage of Section 230 immunity.

B. Explicitly committing to the principle of collective responsibility and incentivizing intervention.

Many harmful acts are only possible with the participation of multiple actors with various motivations. The doctrines of aiding and abetting, complicity, and conspiracy all reflect the insight that third parties who assist, encourage, ignore, or contribute to the illegal actions of another person can and should be held responsible for their contributions to the harms that result, particularly if those third parties benefited in some material way from that

contribution. While U.S. law, unlike the law of some countries, does not impose a general duty to aid, it does recognize the concept of collective responsibility. Third parties can be held both criminally and civilly liable for the actions of other people for harmful acts they did not cause but did not do enough to prevent.

Among the justifications for third-party liability in criminal and civil law is that this liability incentivizes responsible behavior. Bartenders who serve alcohol to obviously inebriated patrons can be sued if those patrons go on to cause car accidents; grocery stores can be held accountable for failing to clean up spills that lead to slip and falls; employers can be liable for failing to respond to reports of sexual harassment. Such entities are often said to have breached a "duty of care," and imposing liability is intended to give them incentive to be more careful in the future. It is a central tenet of tort law that the possibility of such liability incentivizes individuals and industries to act responsibly and reasonably.

Conversely, grants of immunity from such liability risk encouraging negligent and reckless behavior. The immunity granted by Section 230 does just that, despite the evocative title of its operative clause, "Protection for 'Good Samaritan' blocking and screening of offensive material." This title suggests that Section 230 is meant to provide "Good Samaritan" immunity in much the same sense as "Good Samaritan" laws in physical space. Such laws do not create a duty to aid, but instead provide immunity to those who attempt in good faith and without legal obligation to aid others in distress. While Good Samaritan laws generally do not require people to offer assistance, they encourage people to assist others in need by removing the threat of liability for doing so.

Subsection (c)(2) of Section 230 is a Good Samaritan law in a straightforward sense: it assures providers and users of interactive computer services that they will not be held liable with regard to 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" or "taken to enable or make available

to information content providers or others the technical means to restrict access" to such material. Importantly, because most interactive computer service providers are private entities, their right to choose whether to carry, promote, or associate themselves with speech is not created by Section 230, but by the First Amendment. Subsection (c)(2) merely reinforces this right by making it procedurally easier to avoid specious lawsuits.

On the other hand, Subsection 230(c)(1)'s broad statement that "No 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," has been interpreted in ways directly at odds with Good Samaritan laws, as well as with a host of other legal principles and settled law. Where (c)(2) offers immunity to interactive computer service providers in exchange for intervening in situations where they have no duty of care, (c)(1) has been read to provide the same immunity to providers who do nothing at all to stop harmful conduct – and, even more perversely, extends that same immunity to providers who actively profit from or solicit harmful conduct. Section 230(c)(1) has been invoked to protect message boards like **8chan** (now 8kun), which provide a platform for mass shooters to spread terrorist propaganda, online firearms marketplaces such as **Armslist**, which facilitate the illegal sale of weapons used to murder domestic violence victims, and to classifieds sites like **Backpage** (now defunct), which was routinely used by sex traffickers to advertise underage girls for sex.

In subsidizing platforms that directly benefit from illegal and harmful conduct, Section 230(c)(1) creates a classic "**moral hazard**," ensuring that the multibillion-dollar corporations that exert near-monopoly control of the Internet are protected from the costs of their risky ventures even as they reap the benefits. Given that the dominant business model of websites and social media services is based on advertising revenue, they have no natural incentive to discourage abusive or harmful conduct: "**abusive posts still bring in considerable ad revenue… the more content that is posted, good or bad, the more ad money goes into their coffers**."

Online intermediaries who do not voluntarily intervene to prevent or alleviate harm inflicted by another person are in no sense "Good Samaritans." They are at best passive bystanders who do nothing to intervene against harm,

and at worst, they are accomplices who encourage and profit from harm. Providing them with immunity flies in the face of the longstanding legal principle of collective responsibility that governs conduct in the physical world. In physical spaces, individuals or businesses that fail to "take care" that their products, services or premises are not used to commit wrongdoing can be held accountable for that failure. There is no justification for abandoning this principle simply because the conduct occurs online.

Creating a two-track system of liability for offline and online conduct not only encourages illegality to move online, but also **erodes** the rule of law offline. Offline entities can plausibly complain that the differential treatment afforded by broad interpretations of Section 230 violates principles of fairness and equal protection, or to put it more bluntly: if they can do it, why can't we? There is a real risk that Section 230's abandonment of the concept of collective responsibility will become the law offline as well as on.

To undo this, Section 230 (c)1 should be further amended to clarify that the prohibition against treating providers or users of interactive computer services as a publisher or speaker should only apply to speech *wholly provided by another information content provider, unless such provider or user intentionally encourages, solicits, or generates revenue from this speech.* In addition, a new subsection should be added to Section 230 to explicitly exclude from immunity intermediaries who exhibit deliberate indifference to unlawful content or conduct.

The revised version of Section 230(c) would read:

> **(1) Treatment of publisher or speaker**
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any ~~information~~ speech wholly provided by another information content provider, unless such provider or user intentionally encourages, solicits, or generates revenue from this speech.
>
> **(2) Civil liability**
> No provider or user of an interactive computer service shall be held liable on account of-

(A) 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; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1);1

(3) Limitations. The protections of this section shall not be available to a provider or user who manifests deliberate indifference to unlawful material or conduct.

2. Instruct Congress to pass clear and effective legislation addressing severe online harms disproportionately targeted at women and minorities, including nonconsensual pornography, sextortion, doxing, and deep fakes.

The new administration should call for the passage of federal legislation addressing new and highly destructive forms of technology-facilitated abuse. Doing so will ensure that victims of these abuses will have a path to justice with or without Section 230 reform, as Section 230 does not apply to violations of federal criminal law.

Victims of online abuse are not safe on or offline. They suffer anxiety, severe emotional distress, and damage to their reputations, intimate relationships, and employment and educational opportunities. Some victims are forced to relocate, change jobs, or change their names. Some have committed suicide.

In addition to inflicting economic, physical, and psychological harms on victims, unchecked online abuse also inflicts free speech harms. Online abuse, especially online sexual abuse, silences victims. To avoid further harassment and threats to themselves and their families, targeted individuals delete their social media accounts, cancel speaking engagements, and refrain from engaging in public discourse. Many alter their professional

choices, including **journalists** who feel compelled to refrain from reporting on controversial topics and politicians forced to **leave office** due to intimidation.

In other words, the failure to regulate online abuse chills speech. The corollary of this observation is that regulation is sometimes necessary to encourage speech. According to a **2017 study** by Jonathon Penney, regulating online abuse "may actually facilitate and encourage more speech, expression, and sharing by those who are most often the targets of online harassment: women." Penney suggests that when women "feel less likely to be attacked or harassed," they become more "willing to share, speak, and engage online." Knowing that there are laws criminalizing online harassment and stalking "may actually lead to more speech, expression, and sharing online among adult women, not less." As expressed in the title of a **recent article** co-authored by Penney and Danielle Keats Citron, sometimes "law frees us to speak."

Technology-facilitated abuses that have proven particularly destructive include nonconsensual pornography (also known as "revenge porn"), sextortion (a form of blackmail in which sexual information or images are used to extort sexual acts and/or money from the victim), doxing (the publication of private or personally identifying information, often with malicious intent), and so-called "deep fakes" (the use of technology to create false visual and audio material indistinguishable from authentic visual and audio representations of individuals). Fortunately, strong federal legislation has already been drafted on the first three issues, and there are strong efforts in process to address the fourth.

The administration should direct Congress to pass the Stopping Harmful Image Exploitation and Limiting Distribution (SHIELD) Act of 2019 (S.2111/H.R.2896), sponsored by Senator Kamala Harris and Congresswoman Jackie Speier, which would make it a crime to knowingly distribute or threaten to distribute private, sexually explicit visual material of an individual, when the distributor knows or recklessly disregards whether the depicted individual has a reasonable expectation of privacy and has not consented

to the distribution, and has no reasonable belief that distribution touches a matter of public concern.

The administration should also call upon Congress to pass the Online Safety Modernization Act of 2017 (H.R.3067), sponsored by Congresswoman Katherine Clark, which would prohibit multiple forms of online abuse, which the bill refers to as "cybercrimes against individuals." These include coercion of sexual acts, sexual contact, and the production of sexually explicit visual depictions; coercion or extortion involving threats to publish sexually explicit visual depictions; the reporting of false or misleading information to initiate an emergency law enforcement response; and the publication of personally identifiable information of another person to threaten, intimidate, harass, or cause other harm. The Act also requires the Department of Justice to develop a national strategy to reduce, investigate, track, and prosecute cybercrimes against individuals, as well as providing personnel, training, state and local grants towards this goal, and requires the Federal Bureau of Investigation to create a category, in the Uniform Crime Reports, for an offense that constitutes a cybercrime against individuals.

The administration should additionally direct Congress to draft and enact a statute criminalizing so-called "deep fakes." The statute should target a narrow category of digital forgeries, defined as audiovisual material that has been created or materially altered to falsely appear to a reasonable observer to be an actual record of actual speech, conduct, appearance, or absence of an individual, that is created, distributed, or reproduced with the intent to cause serious harm or with reckless disregard for whether serious harm would result.

3. Appoint a Commissioner on Cyber Abuse and Extremism to work with the National Task Force on Online Harassment and Abuse and to lead research and policy efforts to combat technology-facilitated abuse, with particular focus on the impact on the privacy, free expression, and democratic participation of women, minorities, and other marginalized groups.

The Biden-Harris administration's announcement that it will convene a **National Task Force on Online Harassment and Abuse** to study the connections between sexual harassment and abuse, mass shootings, extremism and violence against women signals that it recognizes how technology-facilitated abuse jeopardizes not only women's physical safety, but also their rights to expression, privacy, education, professional achievement, and civic participation. The administration should appoint a Commissioner on Cyber Abuse and Extremism to work in coordination with this Task Force and to spearhead research and policy efforts to combat technology-facilitated abuses, including sexual harassment and exploitation, radicalization, and mis/disinformation. These efforts should be particularly focused on safeguarding and promoting the privacy, free expression, and democratic participation of women, minorities, and other marginalized groups.

Among the Commissioner's primary areas of focus should be the often-overlooked role that misogyny plays in violent extremism, given that the abuse of women is one of the most common characteristics of mass shooters and other terrorists who are increasingly radicalized in online spaces. Understanding the interplay of technology, firearms, and misogyny is vital for combating not only violence against women, but violence against society as a whole. The Commissioner should also make recommendations regarding the responsibility that social media and other internet platforms share in the encouragement and amplification of abuse.

OBJECTIONS AND CHALLENGES

A. Danger to Free Speech.

Some claim that any reform of Section 230 jeopardizes free speech in a larger sense, even if not strictly in the sense of violating the First Amendment. Of course, free speech is a cultural as well as a constitutional matter. It is shaped by non-legal as well as legal norms, and tech companies play an outsized role in establishing those norms. There is indeed good reason to be concerned

about the influence of tech companies and other powerful private actors over the ability of individuals to express themselves. This is an observation scholars and advocates who work on online abuse issues have been making for years—that some of the most serious threats to free speech come not from the government, but from non-state actors. Marginalized groups in particular, including women and racial minorities, have long battled with private censorial forces as well as governmental ones.

But the unregulated internet—or rather, the selectively regulated internet—is exacerbating, not ameliorating, this problem. The current model shielding platforms from liability may ensure free speech for the privileged few; protecting free speech for all will require legal reform.

B. Piecemeal Approach.

Some reformers maintain that the best way to reform Section 230 is to create explicit exceptions from its legal shield for certain types of particularly egregious behavior. This was the approach taken in the controversial 2016 Stop Enabling Sex Traffickers Act (SESTA), which amended Section 230 by rendering websites liable for knowingly hosting sex trafficking content. But Section 230's problems are structural, and its flaws **cannot be cured** through a piecemeal approach. The exceptions approach is inevitably underinclusive, establishing an arbitrary hierarchy of harms that creates troubling normative and fairness implications. Such an approach also requires Section 230's exceptions to be regularly updated, an impractical option given the glacial pace of congressional efforts and partisan deadlock.

CONCLUSION

The problem of platform liability brings to mind a popular expression often attributed to the 18th-century statesman Edmund Burke: "The only thing necessary for the triumph of evil is for good men to do nothing." While Burke did not author those words, he did offer a similarly wise sentiment that can help guide efforts to fix what the law of cyberspace has broken: "When bad men combine, the good must associate; else they will fall one by one, an unpitied sacrifice in a contemptible struggle."

ABOUT THE AUTHOR

Dr. Mary Anne Franks is Professor of Law and Dean's Distinguished Scholar at the University of Miami School of Law, where she teaches First Amendment law, Second Amendment law, criminal law and procedure, and law and technology. She serves as the President and Legislative and Tech Policy Director of the nonprofit organization Cyber Civil Rights Initiative and is the author of the award-winning book *The Cult of the Constitution: Our Deadly Devotion to Guns and Free Speech* (2019).
Twitter handle: @ma_franks