Mark R. Warner
US Senator from the Commonwealth of **Virginia**

The SAFE TECH Act (Safeguarding Against Fraud, Exploitation, Threats, Extremism and Consumer Harms Act)

The internet and web have changed dramatically in the 25 years since the enactment of Section 230. This period has seen a shift from a largely decentralized constellation of interest- and affinity-based message boards and online forums (frequently predicated on user-driven moderation), personal and hobbyist websites, and user-driven search and discovery to a more centralized model, mediated by large commercial providers. Entire swathes of economic activity once operated exclusively *offline* have now become internet-enabled, and in many cases predominantly *online*-based and platform-mediated – but (in large measure because of Section 230) without many of the consumer safeguards and civil rights protections that have long attached to these activities and functions.

An original impetus for Section 230 was a state court ruling in 1995 that many consider flawed (and unlikely to have been adopted more broadly), holding an online bulletin board was liable for a user's defamatory post *because* it moderated some content and had established content guidelines – signifying editorial control. Section 230 provides "interactive computer services" with immunity from liability for the content of their users. And – reversing the poorly-reasoned 1995 case – ensures that these providers retain this broad immunity even when they engage in moderation efforts of user content.

While the law was meant to encourage service providers and users to adopt tools to screen and filter objectionable content, it has instead conferred sweeping immunity on online providers even when they do nothing to address misuse of their products, leaving consumers who suffer harm with little – if any – recourse.

A chilling example of this occurred with the popular online dating service Grindr, which successfully invoked the law to protect its ability to do *nothing* in the face of a court injunction – even as its tools were a key enabler of cyber-stalking and harassment impersonation campaign that threatened lives. According to leading organizations focused on ending intimate partner violence, such online impersonation efforts are widespread – with little that victims can do to address these abusive activities.

The internet has in parallel become a new battleground in the fight to protect hard-won civil rights. As legal scholar Olivier Sylvain has noted, even as online intermediaries directly shape the form and substance of user (both consumer and advertiser) interactions, Section 230 provides companies a "free pass for enabling unlawful discriminatory conduct" such as racial and gender discrimination in the context of short-term housing rentals, employment advertisements and more.

Separately, the multi-billion dollar online advertising market has become a focal point for scam artists and fraudsters, with online intermediaries turning a blind eye to the ways in which their tools are repeatedly misused by bad actors to prey on vulnerable consumers – steering them to bogus health care plans, exposing them to countless financial frauds, exploiting those seeking medical care, including drug treatment and reproductive services, and more. With many of these frauds perpetrated by criminal actors overseas, consumers have limited recourse in the wake of platform inaction.

Service providers' disregard of the misuse of their platforms has produced more than just consumer harm: in many cases, continued – and reckless – inaction of platforms has facilitated pervasive online harassment of BIPOC, LGBTQ+ and religious-minority users. With abusers often shielded by online anonymity and platforms' neglect of meaningful reporting tools, victims are in large measure left to fend for themselves. A law that was supposed to promote online speech has instead helped bad actors intimidate, bully, and hound some of the most vulnerable and marginalized users from participation in the increasingly online public sphere.

Platforms enjoy legal immunity even where their services are openly used to perpetrate foreseeable and preventable violence. A platform that hosts organizing efforts for armed militia groups making direct calls for violence faces no legal consequences for its actions, even when reported by users hundreds of times in advance of the tragic events. Similarly, even as platforms repeatedly provide the recruiting and organizing tools for violent extremist groups – including serving as the organizing infrastructure for those engaged in the Capitol siege that led to the deaths of multiple Capitol Police officers – Section 230 shields platforms from any wrongful death action that might seek to hold them responsible for their reckless and sustained inaction as their tools are openly and repeatedly misused.

The SAFE TECH Act would force online service providers to finally address these problems or face potential civil liability. It does so by making clear that Section 230:

• **Doesn't apply to ads or other paid content** – ensuring that platforms cannot continue to profit as their services are used to target vulnerable consumers;

• **Doesn't bar injunctive relief** – allowing victims to seek court orders where misuse of a provider's services is likely to cause irreparable harm;

• **Doesn't impair enforcement of civil rights laws** – maintaining the vital and hard-fought protections from discrimination even when activities or services are mediated by internet platforms;

• **Doesn't interfere with laws that address stalking/cyber-stalking or harassment and intimidation on the basis of protected classes**– ensuring that victims of abuse and targeted harassment can hold platforms accountable when they directly enable harmful activity;

• **Doesn't bar wrongful death actions** – allowing the family of a decedent to bring suit against platforms where they may have directly contributed to a loss of life;

• **Doesn't bar suits under the Alien Tort Claims Act** – potentially allowing victims of platform-enabled human rights violations abroad (like the survivors of the Rohingya genocide) to seek redress in U.S. courts against U.S.-based platforms.

These changes to Section 230 do not guarantee that platforms will be held liable in all, *or even most*, cases. Proposed changes do not subject platforms to strict liability; and the current legal standards for plaintiffs still present steep obstacles. Rather, these reforms ensure that victims have an *opportunity* to raise claims without Section 230 serving as a categorical bar to their efforts to seek legal redress for harms they suffer – even when directly *enabled* by a platform's actions or design.

The SAFE TECH Act reaffirms that vital consumer safeguards and civil rights protections don't end when activity moves online, preventing online providers from continuing to externalize the costs of their scale and mismanagement on the public.

Mark R. Warner
US Senator from the Commonwealth of **Virginia**

The SAFE TECH Act
Frequently Asked Questions

Q: What does Section 230 of the Communications Decency Act do?

A: Section 230 grants two forms of immunity to "interactive computer services"—a term that covers a broad range of companies spanning internet platforms like Facebook and YouTube to ISPs, web hosting services, and others.

- Section 230(c)(1) grants immunity to interactive computer services for "information" provided by third parties. It is this provision that ensures Facebook is not liable for a defamatory statement posted by one of its users. Courts have interpreted the word "information" broadly to cover commercial activity and other online (or online-enabled) conduct.

- Section 230(c)(2) grants immunity to interactive computer services for taking action to remove content or restrict access to it if they consider the content to be "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." This provision allows YouTube to take down videos claiming the 2020 presidential election was fraudulent without fear of being sued by the users posting the videos. It also empowers interactive computer service providers to engage in moderation without fear that their moderation will be used to classify them as publishers of the third-party content.

Q: Why was Section 230 enacted?

A: Enacted in 1996 as a largely-overlooked amendment to the larger Telecommunications Act of 1996, Section 230 was a response to the New York state court decision Stratton Oakmont v. Prodigy. In that case, the court found Prodigy liable for a defamatory statement posted by an unknown user to one of its online bulletin boards. The court reasoned that because Prodigy moderated its bulletin boards to remove content it deemed offensive or in bad taste, it was akin to a publisher and therefore responsible for all content posted by third parties.

Section 230 was a rebuke of that decision and ensured that no "interactive computer service" would be treated as the publisher or speaker of content provided by a third party, even if they engaged in moderation activity.

Q: Does Section 230 currently contain any exceptions?

A: From its inception, Section 230 contained exceptions for federal criminal law, intellectual property law, and the Communications Privacy Act of 1986. In 2018, the Stop Enabling Sex Traffickers Act ("SESTA") and Allow States and Victims to Fight Online Sex Trafficking Act ("FOSTA") were signed into law, creating an additional exception for sex trafficking laws. Over time, Congress has considered additional exceptions to Section 230, including for child sexual abuse material ("CSAM").

Q: What does the SAFE TECH Act do?

A: The SAFE TECH Act reforms Section 230 to address key areas in which the law has been abused by platforms to evade responsibility for real-world harms they have directly enabled. Specifically, the bill makes clear that Section 230:

• **Doesn't apply to ads or other paid content** – ensuring that platforms cannot continue to profit as their services are used to target vulnerable consumers;

• **Doesn't bar injunctive relief** – allowing victims to seek court orders where misuse of a provider's services is likely to cause irreparable harm;

• **Doesn't impair enforcement of civil rights laws** – maintaining the vital and hard-fought protections from discrimination even when activities or services are mediated by internet platforms;

• **Doesn't interfere with laws that address stalking/cyber-stalking or harassment and intimidation on the basis of protected classes**– ensuring that victims of abuse and targeted harassment can hold platforms accountable when they directly enable harmful activity;

• **Doesn't bar wrongful death actions** – allowing the family of a decedent to bring suit against platforms where they may have directly contributed to a loss of life;

• **Doesn't bar suits under the Alien Tort Claims Act** – potentially allowing victims of platform-enabled human rights violations abroad (like the survivors of the Rohingya genocide) to seek redress in U.S. courts against U.S.-based platforms.

Q: Won't removing Section 230 immunity bring back the perverse incentive structure Section 230 was meant to address and actually lead to less content moderation?

A: No. Section 230 effectively cut off the development of case law for the past 25 years based on the flawed reasoning of a single state court judge. By peeling back Section 230 immunity for particularly serious harms—such as civil rights violations, stalking, and harassment—internet platforms will be incentivized to ramp up their address problems in these areas, problems that have otherwise been allowed to fester and grow without exposure to potential liability. These reforms do not render ICS providers liable for all – or even most – third-party content, including where they engage in moderation activity. Nor do these reforms alter the already-steep hill plaintiffs must already climb. Rather, these reforms allow victims an opportunity to seek redress where they can potentially show that a platform has directly contributed to their injury.

Q: Will making internet platforms liable for third-party content lead internet platforms to overreach in their content moderation efforts thereby chilling speech from the very groups you're looking to protect?

A: No. The SAFE TECH Act was developed in partnership with, and has the strong support of, a wide array of civil rights groups. We need to recognize that threats, harassment, and targeted intimidation silence the voices of far too many racial minorities, women, and other marginalized groups by driving them from social media and other online platforms. Under the status quo, platforms have been able to ignore these harms – even where their continued inaction, and even their product design, contributes to these injustices. As these online harms spread to the real world—in places like Charlottesville, Kenosha, and at the U.S. Capitol—their negative impact has only become more unmistakable. The SAFE TECH Act simply allows victims an opportunity to hold platforms accountable when their deliberate inaction or product design decisions produce real-world harm, making the online world a more open and welcoming environment for all to participate.

Q: Will exposing small tech companies and startups to liability and increased litigation costs drive them out of business and simply entrench the dominant player (e.g., Google, Facebook)?

A: This concern is gravely exaggerated. As an initial matter, smaller players do not have the reach of the Googles and Facebooks of the world and, as a result, are less likely to cause significant harm. Moreover, potential plaintiffs are unlikely to bring an action against a small tech company or startups out of fear being able

to collect sufficient damages to make the effort and cost of litigation worthwhile. Indeed, in many cases plaintiffs' attorneys would not even take these cases given the low likelihood of meaningful damages. In addition, a string of judicial decisions on standing requirements over the last 10 years, along with a range of tort reforms enacted by state legislatures (including anti-SLAPP laws to penalize frivolous or bad faith lawsuits), have significantly altered the legal landscape since Section 230 was enacted in 1996.

More importantly, things like protecting civil rights and preventing harassment *should* be built into internet platforms ***by design***. Today's online giants claim that their massive scale makes it too difficult to effectively moderate content – a social cost borne by users and vulnerable communities. Had these companies been exposed to potential liability from their inception, in many cases they would have designed their platforms to address (and avert) misuse and harm stemming from them.

Q: What is the scope of the carve-out for paid content? Does it cover anything beyond paid advertisements?

A: The SAFE TECH Act makes clear that Section 230 immunity does not apply to ***any*** paid content. This would include advertisements as well as things like marketplace listings.

Q: Why is a carve-out for antitrust laws necessary?

A: Internet platforms and other tech companies have pushed the bounds of Section 230 in an effort to immunize themselves from all manner of activity. Just last year, a leading cyber-security firm claimed Section 230 immunized it against a claim it had engaged in anticompetitive conduct to harm a competitor and pursued its claim all the way to the Supreme Court. With federal and state antitrust enforcers turning their eyes to dominant technology platforms (including the ways in which they shut off access to downstream competitors based on anti-competitive motives), it is important to make clear that Section 230 does not provide immunity for anticompetitive conduct.

Q: Will the SAFE TECH Act break the internet?

A: No! The internet was a far different place when Section 230 was passed. The scope, influence, and impact of modern internet platforms were unimaginable in 1996. Like all regulation, Section 230 must be updated to address the current state of affairs – including the unintended consequences of the law. The SAFE

TECH Act brings Section 230 into the modern age by addressing those areas in which the law has been abused by platforms—such as civil rights, stalking, and harassment—in a targeted way. It is also important to remember, that even with the changes proposed in the SAFE TECH Act, Section 230 does not impose liability on anyone. There must still be a violation of some law and plaintiffs must still prove causation, harm, and damages. And the application of that law to an internet platform still cannot run afoul of the First Amendment.