Hearing Before the Subcommittee on Communications, Technology, Innovation, and the Internet, United States Senate Committee on Commerce, Science, and Transportation

"The PACT Act and Section 230: The Impact of the Law that Helped Create the Internet and an Examination of Proposed Reforms for Today's Online World"

Testimony of Former U.S. Rep. Chris Cox
Author and Co-Sponsor with Sen. Ron Wyden, Section 230

July 28, 2020
106 Dirksen Senate Office Building
Washington, D.C.

TESTIMONY OF FORMER U.S. REPRESENTATIVE CHRIS COX
BEFORE THE SUBCOMMMITTEE ON COMMUNICATIONS, TECHNOLOGY,
INNOVATION, AND THE INTERNET,
U.S. SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
"THE PACT ACT AND SECTION 230: THE IMPACT OF THE LAW
THAT HELPED CREATE THE INTERNET AND AN EXAMINATION OF PROPOSED REFORMS
FOR TODAY'S ONLINE WORLD"
JULY 28, 2020

Chairman Thune, Ranking Member Schatz, and Members of the Subcommittee, thank you for the invitation to testify on the history of Section 230 and its application by the courts over the last quarter century. This experiential base is an important starting point as you consider ways to ensure that platforms are accountable for their content moderation practices, and what legislative measures, from transparency to accountability tools, can empower consumers online.

My abiding interest in this subject dates, of course, to some twenty-four years ago when I joined then-Rep. Ron Wyden in writing what today is known as Section 230. In the intervening quarter century I have followed the developments in the case law, sometimes with awe and occasionally with disappointment. The views I express today are my own, and not necessarily those of NetChoice, on whose board I serve, or of Morgan, Lewis & Bockius.

Introduction

As we consider the issues surrounding free expression and content moderation on the internet, it is worth asking: what would our world be like without Section 230?

This is an important question because, to a degree most of us fail to recognize, we take its many benefits for granted. An endless variety of useful and important content on the internet is supplied not by websites or social media platforms, but by their millions of users who create the content themselves and freely share it. Without Section 230, millions of American websites—facing unlimited legal liability for what their users create—would not be able to host user-generated content at all.

In this way, moreover, Section 230 facilitates every individual's ability to publish their own content on the internet. The wide variety of online forums for posting user-created content is the direct result of the protection from liability for the host sites that Section 230 affords.

At the same time that Section 230 has enabled an endless diversity of voices to reach far greater audiences than was ever possible before, this same law has helped websites to maintain civility and fair play through the application of bespoke standards of content moderation. In contrast to other nations, in the United States the government does not dictate what can be published on the internet and who can publish it. The proliferation of websites, each free to adopt their own rules of the road, has simultaneously provided unparalleled opportunities for any individual to reach millions of people around the world—and the

means by which offensive online conduct including bullying and obscenity, as well as outright criminal activity, can be restricted without fear of legal liability.

Before the enactment of Section 230, internet platforms faced a terrible dilemma. If they sought to enforce even minimal rules of the road in order to maintain civility and keep their sites free from obscenity and obnoxious behavior, they became unlimitedly liable for all of the user-created content on their site.[1] On the other hand, if the website followed an "anything goes" business model, with no content moderation whatsoever, then it could completely avoid that liability.[2] From the perspective of any internet platform that attempted to maintain a family-friendly site, it was a classic case of "no good deed goes unpunished."

Section 230 eliminated the perverse incentive for "anything goes." By imposing liability on criminals and tortfeasors for their own wrongful communications and conduct, rather than shifting that liability to a website that did not in any way participate in the wrongdoing, it freed each website to clean up its corner of the internet. No longer would being a "Good Samaritan" buy trouble.

In an imagined future world without Section 230, where websites and internet platforms again face enormous potential liability for hosting content created by others, there would again be a powerful incentive to limit that exposure. Online platforms could accomplish this in one of two ways. They could strictly limit user-generated content, or even eliminate it altogether; or they could adopt the "anything goes" model that was the way to escape liability before Section 230 existed.

We would all be very much worse off were this to happen. Without Section 230's clear limitation on liability it is difficult to imagine that most of the online services on which we rely every day would even exist in anything like their current form.

As Congress considers whether to amend Section 230, therefore, it is important to keep in mind the many aspects of the modern internet we take for granted, and that are dependent upon Section 230's protections. Compromising those protections risks a wide array of unintended consequences. Among these are loss of much of the rich content provided every day by millions of individual content creators, loss of the ability to use social media for real time communication with friends and family, loss of opportunities for diverse voices to reach broad audiences throughout the nation and across the planet, and damage to e-commerce and the continued technological development of the internet.

In the 21st century, Section 230's protection of website operators from liability for content created by their users operates as an essential buttress of free expression. It is the key to millions of Americans' ability to share news and views and gain instant access to a wide range of informational and educational resources. It is the foundation supporting e-commerce sites such as Yelp, eBay, Facebook, Wikipedia, Amazon, Twitter, and the entire Web 2.0 revolution whereby thousands of innovative platforms offer a range of useful services powered by user-generated content. From user-created reviews of products and services, to educational videos, to online resources that help locate loved ones after natural disasters, to the many online services that have come to the rescue of millions of Americans quarantined or in self-isolation

[1] *Stratton Oakmont v. Prodigy Servs. Co*., 1995 WL 323710 (N.Y.Sup.Ct. May 24, 1995).
[2] *Cubby, Inc. v. CompuServe, Inc*., 776 F. Supp. 135, 140 (S.D.N.Y. 1991).

during the Covid pandemic, all of the rich variety now available at our fingertips is precisely what Section 230 was designed to facilitate.

But while Section 230 has been a boon to users of the internet and to the continued technological and commercial development of the internet itself, it is not a panacea. We are all familiar with the many pathologies that continue to fester in corners of the dark web, and that too often leach onto the mainstream internet websites and platforms we rely on every day. Continued challenges to a free and open internet include the threat of hidden platform "censorship" and undisclosed viewpoint discrimination; "fake news" and content manipulation by bad actors; defamation, cyberstalking, and revenge porn; fraud on consumers; internet-facilitated criminal gang activity; cross-border terrorism; child sexual abuse and sex trafficking; and widespread censorship and social control by dictatorships and authoritarian governments including not only Russia and China, but scores of other nations besides.

Section 230 has not prevented these affronts, but neither is it the cause of them. In many cases, it has helped mitigate their consequences. Preserving the law's benefits for internet users, society, and the nation's economy should remain an overarching objective of any legislation to address the many looming concerns across the rapidly-evolving landscape of the internet.

In that respect, we will be well advised to recognize the danger of unintended consequences that would accompany efforts to reopen Section 230 to further amendment. There are many competing interests at stake, both commercially and politically, in the constellation of issues affected by Section 230. As each of you is fully aware, the various criticisms of Section 230 come from disparate quarters, and are based on radically different rationales. For example, while some critics demand more robust content moderation, their political opposites demand less interference with user-created content. The process of turning a bill into law in these circumstances will require potentially trenchant compromises.

The multiplicity of stakeholders, including competing business interests, affected by any new legislation governing activity on the internet—not to mention the many different committees that will be involved in both the House and Senate, and the inevitable need to compromise among them in order for a bill to make it through the entire process—means that you may not recognize your legislative handiwork in the final product. So even though it is possible to imagine that a "perfect" bill might emerge from the Commerce Committee that would clarify and improve Section 230 while preserving all of its benefits, the legislative process that will inevitably follow is likely to adulterate that "perfection" and potentially threaten the essential elements of Section 230 that make it work. This very real risk to the many societal benefits that a majority of Congress still believes flow from Section 230 is worth considering before opening what could be a Pandora's box.

Background and Legislative History of Section 230

Section 230 was signed into law 24 years ago, in 1996.[3] When my colleague Ron Wyden (D-OR) and I conceptualized the law in 1995, roughly 20 million American adults had access to the internet, compared to 7.5 billion today.

[3] 104 P.L. 104, 110 Stat. 56.

Those who were early to take advantage of the opportunity to "surf the web," including many in Congress, quickly confronted this essential aspect of online activity: on each website, many users converge through one portal. The difference between newspapers and magazines, on the one hand, and the World Wide Web (as it was then called), on the other hand, was striking. In the print world, a single staff of human beings reviewed and cataloged editorial content that was then distributed to a large number of passive recipients. The same was true of television and radio. On the web, in contrast, millions of users themselves created content which became accessible to the entire planet immediately. While the volume of users was only in the millions, not the billions as today, it was even then evident to almost every user of the web that no group of human beings would ever be able to keep pace with the growth of content on the internet.

At the time, however, not all in Congress were users of the web who appreciated these fundamentals. The Communications Decency Act ("CDA"), introduced in the Senate by James Exon (D-NE), was premised on the notion that the FBI could filter the web, screening out offensive content. This was a faulty premise based on a fundamental misunderstanding of the scale and the functioning of the internet. Nonetheless, in large part because the stated target of the CDA was pornography, the Senate voted overwhelmingly (the vote was 84-16) in favor of it.[4]

Section 230 was not part of the CDA. Instead, it was a freestanding bill introduced in the House as H.R. 1978, the Internet Freedom and Family Empowerment Act, in June 1995. It was intended as an *alternative* to the CDA. When it was offered as a standalone Cox-Wyden amendment on the House floor during consideration of the Telecommunications Act in August 1995, it was roundly endorsed on both sides of the aisle during debate. At the same time, both Democratic and Republican lawmakers sharply criticized the CDA. They then voted nearly unanimously in favor of the Cox-Wyden amendment, while excluding the CDA from the House version of the Telecommunications Act.

In the conference on what became the Telecommunications Act of 1996 that followed, as is so often the case in legislative compromises between House and Senate, the conferees agreed to include both diametrically opposed bills in the Conference Report. Subsequently, the U.S. Supreme Court gutted the CDA's indecency provisions, which it found violated the First Amendment, giving Rep. Wyden and me the victory we did not at first achieve in conference.[5]

The fundamental flaw of the CDA was its misunderstanding of the internet as a medium. We can now easily see that it would have been impossible for the bulletin boards, chat rooms, forums, and email that were then budding on the web to be screened in any meaningful way by the FBI, or by the operators of individual websites themselves, even at the far lower volumes of traffic that existed then. Worse, if the law were to demand such screening, the fundamental strength of the new medium—facilitating the free exchange of information among millions of users—would be lost.

[4] *Id*.
[5] *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

The *Prodigy* and *CompuServe* cases

The impetus for the Internet Freedom and Family Empowerment Act, today's Section 230, was a New York Superior Court case that I first saw reported in the *Wall Street Journal* in May 1995.[6] It involved one of the leading internet portals of the day. The case concerned an allegedly defamatory bulletin board post on the Prodigy web service by an unknown user. The post claimed that an investment bank and its founder, Jordan Belfort, had committed securities fraud. (The post was not in fact defamatory: Belfort was later convicted of securities fraud, but not before Prodigy had settled the case for a substantial figure. Belfort would achieve further infamy when he became the model for Leonardo DiCaprio's character in "The Wolf of Wall Street.")

By holding Prodigy liable for the allegedly illegal content posted by its user, the New York court established a new precedent with far-reaching consequences.[7] Up until then, the courts had not permitted such claims for third-party liability. In 1991, a federal district court in New York held that CompuServe, another web service similar to Prodigy that hosted a variety of user-created content, was not liable in circumstances very similar to those in the *Prodigy* case. The court reasoned that CompuServe "had no opportunity to review the contents of the publication at issue before it was uploaded into CompuServe's computer banks," and therefore was not subject to publisher liability for the third party content.[8]

But in the 1995 New York Superior Court case, the court distinguished the *CompuServe* precedent. The reason the court offered was that unlike CompuServe, Prodigy sought to impose general rules of civility on its message boards and in its forums. While Prodigy had even more users than CompuServe and thus even less ability to screen material on its system, the fact it had announced rules of the road and occasionally enforced them was the judge's basis for subjecting it to liability that CompuServe didn't face.

The perverse incentive this case established was clear: any provider of interactive computer services should avoid even modest efforts to moderate the content on its site. The inevitable consequences for the future of the internet were equally clear: every website would be incentivized to follow CompuServe's model of "anything goes." Unless corrective action were taken the internet, already beginning to show some erosion in standards of public discourse that must inevitably arise when thousands and then millions of people engage in uninhibited public expression on any topic, would quickly become nothing but a sewer. When I read about this decision, I immediately set to work on drafting a bill to head off its predictable bad consequences.

Creating Section 230 and its goals

The first person I turned to as a legislative partner on my proposed bill was then-Rep. Ron Wyden (D-OR). We had previously agreed to seek out opportunities for bipartisan legislation. As this was a novel question of policy that had not hardened into partisan disagreement (as was too often the case with so

---

[6] Milo Geyelin, *New York judge rules Prodigy responsible for on-line content*, Wall St. Jo., May 26, 1995.
[7] *Stratton Oakmont v. Prodigy Servs. Co*., 1995 WL 323710 (N.Y.Sup.Ct. May 24, 1995)
[8] *Cubby, Inc. v. CompuServe*, Inc., 776 F. Supp. 135, 140 (S.D.N.Y. 1991) (emphasis added).

many other issues), we knew we could count on a fair consideration of the issues from our colleagues on both sides of the aisle.

For the better part of a year, we conducted outreach and education on the challenging issues involved. In the process, we built not only overwhelming support, but also a much deeper understanding of the unique aspects of the internet that require clear legal rules for it to function.

The rule established in the Internet Freedom and Family Empowerment Act,[9] which we introduced in June 1995, was crystal clear: the government would impose liability on criminals and tortfeasors for wrongful conduct. It would not shift that liability to third parties, because doing so would directly interfere with the essential functioning of the internet.

Rep. Wyden and I were well aware that whether a person is involved in criminal or tortious conduct is in every case a question of fact. Simply because one operates a website, for example, does not mean that he or she cannot be involved in lawbreaking. To the contrary, as the last two decades of experience have amply illustrated, the internet—like all other means of telecommunication and transportation—can be and often is used to facilitate illegal activity.

Section 230 was written, therefore, with a clear fact-based test:

- Did the person create the content? If so, that person is liable for any illegality.
- Did someone else create the content? Then that someone else is liable.
- Did the person do anything to develop the content created by another, even if only in part? If so, the person is liable along with the content creator.

The plain language of the statute directly covers the situation in which someone (or some company) is only partly involved in creating the content. Likewise, it covers the situation in which they did not create the content but were, at least in part, responsible for developing it. In both cases, Section 230 comes down hard on the side of law enforcement. A website operator involved only in part in content creation, or only in part in the development of content created by another, is nonetheless treated the same as the content creator.

Here is the precise language of section 230 in this respect:

> The term "information content provider" means any person or entity that is responsible, in whole or *in part*, for the creation *or development of* information provided through the Internet ….[10]

[9] Internet Freedom and Family Empowerment Act, H.R. 1978, 104 Cong. (1995).
[10] 47 USC § 230(f) (emphasis added).

These words in Section 230—"in part" and "development of"—are the most important part of the statute. That is because in enacting Section 230, it was not our intent to create immunity for criminal and tortious activity on the internet. To the contrary, our purpose (and that of every legislator who voted for the bill) was to ensure that innocent third parties will not be made liable for unlawful acts committed wholly by others.

If an interactive computer service becomes complicit, in whole or in part, in the creation of illicit content—even if only by partly "developing" the content—then it is entitled to no Section 230 protection. Rep. Wyden and I knew that, in light of the volume of content that even in 1995 was crossing most internet platforms, it would be unreasonable for the law to presume that the platform will screen all material. We also well understood the corollary of this principle: if in a specific case a platform actually did review material and edit it, then there would be no basis for assuming otherwise. As a result, the plain language of Section 230 deprives such a platform of immunity.

We then created an exception to this deprivation of immunity, for what we called a "Good Samaritan."[11] If the purpose of one's reviewing content or editing it is to restrict obscene or otherwise objectionable content, then a platform will be protected. Obviously, this exception would not be needed if Section 230 provided immunity to those who only "in part" create or develop content.

The importance of Section 230 for user-generated content

In simplest terms, Section 230 protects website operators that are not involved in content creation from liability for content created by third party users. Without it, websites would be exposed to lawsuits for everything from users' product reviews to book reviews. Yelp would be exposed to lawsuits for its users' negative comments about restaurants, and Tripadvisor could be sued for a user's disparaging review of a hotel. Any service that connects buyers and sellers, workers and employers, content creators and a platform, victims and victims' rights groups—or provides any other interactive engagement opportunity we can imagine—would face open-ended liability if it continued to display user-created content.

How important is user-created content? Without it, it is hard to imagine how any of us would have made it this far through the Covid quarantines and self-isolation of 2020. Many contending with this year's devastating tornadoes—this is already the deadliest tornado season in the United States since 2011—could not have found their loved ones. This year more than ever, millions of Americans are relying on "how to" and educational videos for everything from healthcare to home maintenance. During the Covid crisis, online access to user-created pre-K, primary, and secondary education and lifelong learning resources has proven a godsend for families across the country.

Over 85% of businesses rely on user-created content on their websites.[12] The vast majority of Americans feel more comfortable buying a product after researching user generated reviews,[13] and over 90% of

[11] 47 U.S.C. § 230 (c)(2)(A).
[12] https://www.semrush.com/blog/50-stats-about-9-emerging-content-marketing-trends-for-2016/
[13] Wu, Y. (2015). What Are Some Interesting Statistics About Online Consumer Reviews? Dr4ward.com. Available at: http://www.dr4ward.com/dr4ward/2013/03/what-are-some-interesting-statistics-about-online-consumer-reviews-infographic.html

consumers find user-generated content helpful in making their purchasing decisions.[14] User generated content is vital to law enforcement and social services. Following the recent rioting in several U.S. cities, social workers have been able to match people with supplies and services to victims who needed life-saving help, directing them with real-time maps.

Protecting the innocent and punishing the guilty

Throughout the history of the internet, Congress has sought to strike the right balance between opportunity and responsibility. Section 230 is such a balance—holding content creators liable for illegal activity while protecting internet platforms from liability for content created entirely by others. At the same time, Section 230 does not protect platforms liable when they are complicit—even if only in part – in the creation or development of illegal content.

The plain language of Section 230 makes clear its deference to criminal law. The entirety of federal criminal law enforcement is unaffected by Section 230. So is all of state law that is consistent with the policy of Section 230.[15]

Still, state law that is inconsistent with the aims of Section 230 is preempted. Why did Congress choose this course? First, and most fundamentally, it is because the essential purpose of Section 230 is to establish a uniform federal policy, applicable across the internet, that avoids results such as the state court decision in *Prodigy*.[16] The internet is the quintessential vehicle of interstate, and indeed international, commerce. Its packet-switched architecture makes it uniquely susceptible to multiple sources of conflicting state and local regulation, since even a message from one cubicle to its neighbor inside the same office can be broken up into pieces and routed via servers in different states.

Were every state free to adopt its own policy concerning when an internet platform will be liable for the criminal or tortious conduct of another, not only would compliance become oppressive, but the federal policy itself could quickly be undone. All a state would have to do to defeat the federal policy would be to place platform liability laws in its criminal code. Section 230 would then become a nullity. Congress thus intended Section 230 to establish a uniform federal policy, but one that is entirely consistent with robust enforcement of state criminal and civil law.

Despite the necessary preemption of inconsistent state laws, every state and every federal prosecutor can successfully target online criminal activity by properly pleading that the defendant was at least partially involved in the creation of illegal content, or at least the later development of it. In all such cases, Section 230 immunity does not apply.

How Section 230 actually works

The importance to millions of Americans of so many topics that Section 230 touches upon either directly or indirectly—for example, the responsibility of social media platforms to their users and the public; the

[14] Kimberly Morrison, "Why Consumers Share User-Generated Content," *Adweek*, May 17, 2016.
[15] 47 USC § 230(e)(3).
[16] *Stratton Oakmont v. Prodigy Servs. Co*., 1995 WL 323710 (N.Y.Sup.Ct. May 24, 1995).

ability of citizens to exercise their First Amendment rights; the ability of law enforcement to track down criminals; the protection of the privacy of every user of the internet—means that almost everyone has an opinion about Section 230 itself. But notwithstanding that Section 230 has become a household name, a complete understanding of how the law functions in practice, and what it actually does, is harder to come by. There are several misconceptions abroad that merit clarification.

Some mistakenly claim that Section 230 prevents action against websites that knowingly engage in, solicit, or support illegal activity. This is simply wrong. But since this claim is often a principal basis for urging amendment of Section 230, it bears repeating that Section 230 provides no protection for any website, user, or other person or business involved *even in part* in the creation *or development* of content that is tortious or criminal.

In the two and a half decades that Section 230 has been on the books, there have been hundreds of court decisions interpreting and applying it. It is now firmly established in the case law that Section 230 cannot act as a shield whenever a website is in any way complicit in the creation or development of illegal content. In the landmark *en banc* decision of the Ninth Circuit Court of Appeals in *Fair Housing Council of San Fernando Valley v. Roommate.com*,[17] which has since been widely cited and applied across the United States, it was held that not only do websites lose their immunity when they merely "develop" content created by others, but participation in others' content creation can be established by the wholly automated features of a website that are coded into its architecture.

There are many examples of courts faithfully applying the plain language of Section 230 to hold websites liable for complicity in the creation or development of illegal third-party content. In its 2016 decision in *Federal Trade Comm'n v. Leadclick Media, LLC*,[18] the Second Circuit Court of Appeals rejected a claim of Section 230 immunity by an internet marketer even though it did not create the illegal content at issue, and the content did not appear on its website. The court noted while this was so, the internet marketer gave advice to the content creators. This made it complicit in the development of the illegal content, and so ineligible for Section 230 immunity.

In *FTC v. Accusearch*,[19] the Tenth Circuit Court of Appeals held that a website's mere posting of content that it had no role whatsoever in creating—telephone records of private individuals—constituted "development" of that information, and so deprived it of Section 230 immunity. Even though the content was wholly created by others, the website knowingly transformed what had previously been private information into a publicly available commodity. Such complicity in illegality was deemed to constitute "development" of the illegal content, as distinguished from its creation.

Other notable examples of this now well-established feature of Section 230 are *Enigma Software Group v. Bleeping Computer*,[20] in which a website was denied immunity despite the fact it did not create the unlawful content at issue, because of an implied agency relationship with an unpaid volunteer who did

[17] 521 F.3d 1157, 1168 (9th Cir. 2008).
[18] 838 F.3d 158 (2d Cir. 2016).
[19] 570 F.3d1187, 1197 (10th Cir. 2009).
[20] 194 F.Supp.3d 263 (2016).

create it; and *Alvi Armani Medical, Inc. v. Hennessey*,[21] in which the court deemed a website to be complicit in content creation because of its alleged knowledge that postings were being made under false identities.

In its 2016 decision in *Jane Doe v. Backpage.com*,[22] however, the First Circuit Court of Appeals cast itself as an outlier, rejecting the holding in *Roommate.com* and its progeny. Instead, it held that "claims that a website facilitates illegal conduct through its posting rules *necessarily* treat the website as a publisher or speaker of content provided by third parties and, thus, are precluded by section 230(c)(1)."[23] This holding completely ignored the definition in subsection (f)(3) of Section 230, which provides that anyone—including a website—can be an "information content provider" if they are "responsible, in whole or in part, for the creation or development" of online content. If a website's posting rules facilitate the development of illegal content, then the website becomes a content provider in its own right, and should be deprived of Section 230 immunity.

Despite the fact that the First Circuit was an outlier in this respect, the notoriety of its decision in the *Backpage* case has given rise to the notion that Section 230 routinely operates as a shield against actual wrongdoing by websites. The opposite is the case. Courts since 2016 have consistently followed the *Roommate* precedent, and increasingly have expanded the circumstances in which they are willing to find websites complicit in the creation or development of illegal content provided by their users.

Ironically, the actual facts in the *Backpage* case were a Technicolor display of complicity in the development of illegal content. Backpage knowingly concealed evidence of criminality by systematically editing its adult ads; it coached its users on how to post "clean" ads for illegal transactions; it deliberately edited ads in order to facilitate prostitution; it prescribed the language used in ads for prostitution; and it moderated content on the site, not for the purpose of removing ads for prostitution, but to camouflage them. It is difficult to imagine a clearer case of complicity "in part, for the creation or development" of illegal content.

Happily, even within the First Circuit, this mistake has now been rectified. In the 2018 decision in *Doe v. Backpage.com*,[24] a re-pleading of the original claims by three new Jane Doe plaintiffs, the court held that allegations that Backpage changed the wording of third-party advertisements on its site were sufficient to deem it an information content provider, and thus ineligible for Section 230 immunity. Much heartache could have been avoided had these allegations concerning Backpage's complicity been sufficiently pleaded in the original case,[25] and had the court reached this sensible and clearly correct decision on the law in the first place.

---

[21] 629 F. Supp. 2d 1302 (S.D. Fla. 2008).

[22] *Jane Doe No. 1, et al. v. Backpage.com LLC, et al*., No. 15-1724 (1st Cir. 2016).

[23] *Id.* (emphasis added).

[24] *Doe No. 1 v. Backpage*, 2018 WL 1542056 (D. Mass. March 29, 2018).

[25] Although the plaintiffs disputed this, in the original case the First Circuit pointedly noted that the record before it expressly *did not* allege that Backpage contributed to the development of the sex trafficking content, even "in part." Instead, the argument that Backpage was an "information content provider" under Section 230 was "forsworn" in the district court and on appeal.

Another misguided notion is that Section 230 was never meant to apply to e-commerce. To the contrary, removing the threat to e-commerce represented by the *Prodigy* decision was an essential purpose in the development and enactment of Section 230.

When Section 230 became law in 1996, user-generated content was already ubiquitous on the internet. The creativity being demonstrated by websites and users alike made it clear that online shopping was an enormously consumer-friendly use of the new technology. Features such as CompuServe's "electronic mall" and Prodigy's mail-order stores were instantly popular. So too were messaging and email, which in Prodigy's case came with per-message transaction fees. Web businesses such as CheckFree demonstrated as far back as 1996 that online bill payment was not only feasible but convenient. Prodigy, America Online, and the fledgling Microsoft Network included features we know today as content delivery, each with a different payment system.

Both Rep. Wyden and I had all of these iterations of internet commerce in mind when we drafted our legislation. We made this plain during floor debate.[26]

Yet another misconception about the coverage of Section 230, often heard, is that it created one rule for online activity and a different rule for the same activity conducted offline. To the contrary, Section 230 operates to ensure that like activities are always treated alike under the law.

When Section 230 was written, just as now, each of the commercial applications flourishing online had an analog in the offline world, where each had its own attendant legal responsibilities. Newspapers could be liable for defamation. Banks and brokers could be held responsible for failing to know their customers. Advertisers were responsible under the Federal Trade Commission Act and state consumer laws for ensuring their content was not deceptive and unfair. Merchandisers could be held liable for negligence and breach of warranty, and in some cases even subjected to strict liability for defective products.

In writing Section 230, Rep. Wyden and I, and ultimately the entire Congress, decided that these legal rules should continue to apply on the internet just as in the offline world. Every business, whether operating through its online facility or through a brick-and-mortar facility, would continue to be responsible for all of its legal obligations. What Section 230 added to the general body of law was the principle that an individual or entity operating a website should not, in addition to its own legal responsibilities, be required to monitor all of the content created by third parties and thereby become derivatively liable for the illegal acts of others. Congress recognized that to require otherwise would jeopardize the quintessential function of the internet: permitting millions of people around the world to communicate simultaneously and instantaneously. Congress wished to "embrace" and "welcome" this not only for its commercial potential but also for "the opportunity for education and political discourse that it offers for all of us."[27]

The result is that websites are protected from liability for user-created content, but *only if they are wholly uninvolved in the creation or development of that content*. Today, virtually every brick-and-mortar

[26] S*ee* 141 Cong. Rec. H8468–72, H8478–79 (August 4, 1995).
[27] Id. at H8470.

business of any kind, from newspapers to retailers to manufacturers to service providers, has an internet presence through which it conducts e-commerce. Whether in the offline world or the internet, the same legal rules and responsibilities apply across the board to all.

It is worth debunking three other "creation myths" about Section 230.

The first is that Section 230 was conceived as a way to protect an infant industry. According to this narrative, in the early days of the internet, Congress decided that small startups needed protection. Now that the internet has matured, it is argued, the need for such protection no longer exists; Section 230 is no longer necessary.

As co-author of the legislation, I can verify that this is an entirely fictitious narrative. Far from wishing to offer protection to an infant industry, our legislative aim was to recognize the sheer implausibility of requiring each website to monitor all of the user-created content that crossed its portal each day. In the 1990s, when internet traffic was measured in the tens of millions, this problem was already apparent. Today, in the second decade of the 21st century, the enormous growth in the volume of traffic on websites has made the potential consequences of publisher liability far graver. Section 230 is needed for this purpose now, more than ever.

The second "creation myth" is that Section 230 was adopted as a special favor to the tech industry, which lobbied for it on Capitol Hill and managed to wheedle it out of Congress by working the system. The reality is far different. In the mid-1990s, internet commerce had very little presence in Washington. When I was moved to draft legislation to remedy the *Prodigy* decision, it was based on my reading news reports of the decision. No company or lobbyist contacted me. Throughout the process, Rep. Wyden and I heard barely at all from the leading internet services of the day. This included both Prodigy and CompuServe, whose lawsuits inspired the legislation. As a result, our discussions of the proposed legislation with our colleagues in the House and Senate were unburdened by importunities from businesses seeking to gain a regulatory advantage over their competitors.

I willingly concede that this was, therefore, a unique experience in my lawmaking career. It is also the opposite of what Congress should expect if it undertakes to amend Section 230, given that today millions of websites and more millions of internet users have an identifiable stake in the outcome.

The final creation myth is that Section 230 was part of a grand bargain with Senator James Exon (D-NE), in which his Communications Decency Act aimed at pornography was paired with the Cox-Wyden bill, the Internet Freedom and Family Empowerment Act, aimed at greenlighting websites to enforce content moderation policies without fear of liability. The claim now being made is that the two bills were actually like legislative epoxy, with one part requiring the other. And since the Exon legislation was subsequently invalidated as unconstitutional by the U.S. Supreme Court, so the argument goes, Section 230 should not be allowed to stand on its own.

In fact, the revisionists contend, the primary congressional purpose back in 1996 was not to give internet platforms limited immunity from liability as Section 230 does. Rather, the most important part of the imagined "package" was Senator Exon's radical idea of imposing stringent liability on websites for the

illegal acts of others—an idea that Exon himself backed away from before his amendment was actually passed. Now, a quarter-century after the Supreme Court threw out the Exon bathwater, the neo-speech regulators are urging us to throw out the Section 230 baby along with it.

The reality is far different than this revisionist history would have it. In fact, the Cox-Wyden bill was deliberately crafted as a rebuke of the Exon approach. When it came to the House floor for consideration, speaker after speaker rose to speak in support, and at the same time criticized the Exon approach. Rep. Zoe Lofgren (D-CA), the mother of 10- and 13-year-old children, shared her concerns with internet pornography and noted that she had sponsored legislation mandating a life sentence for the creators of child pornography. But, she emphasized, "Senator Exon's approach is not the right way. … It will not work." It was, she said, "a misunderstanding of the technology."

Rep. Bob Goodlatte, a Virginia Republican, emphasized the potential the internet offered and the threat to that potential from Exon-style regulation. "We have the opportunity for every household in America, every family in America, soon to be able to have access to places like the Library of Congress, to have access to other major libraries of the world, universities, major publishers of information, news sources. There is no way," he said, "that any of those entities, like Prodigy, can take the responsibility to edit out information that is going to be coming in to them from all manner of sources."

In the end, not a single representative spoke against the bill. The final roll call on the Cox-Wyden amendment was 420 yeas to 4 nays. It was a resounding rebuke to the Exon approach in his Communications Decency Act. The House then proceeded to pass its version of the Telecommunications Act—with the Cox-Wyden amendment, and without Exon.

When the House and Senate met in conference on the Telecommunications Act, the House conferees sought to include Cox-Wyden and strike Exon. But political realities as well as policy details had to be dealt with. There was the sticky problem of 84 senators having already voted in favor of the Exon amendment. Once on record with a vote one way—particularly a highly visible vote on the politically charged issue of pornography—it would be very difficult for a politician to explain walking it back. The Senate negotiators, anxious to protect their colleagues from being accused of taking both sides of the question, stood firm. They were willing to accept Cox-Wyden, but Exon would have to be included, too. The House negotiators, all politicians themselves, understood. This was a Senate-only issue, which could be easily resolved by including both amendments in the final product. It was logrolling at its best.

Perhaps part of the enduring confusion about the relationship of Section 230 to Senator Exon's legislation has arisen from the fact that when legislative staff prepared the House-Senate conference report on the final Telecommunications Act, they grouped both Exon's Communications Decency Act and the Internet Freedom and Family Empowerment Act into the same legislative title. So the Cox-Wyden amendment became Section 230 of the Communications Decency Act—the very piece of legislation it was designed to counter. Ironically, now that the original CDA has been invalidated, it is Ron's and my legislative handiwork that forever bears Senator Exon's label.

Measuring the PACT Act and Other Pending Federal Legislation Against the Goals Section 230 Is Meant to Achieve

When Congress enacted what we know today as Section 230 by near-unanimous votes in the House and the Senate, there was broad agreement on several basic principles. Some of these are set forth in the law's preamble; others are set forth in the operational portion of the statute. These basic tenets are as follows:

- The wide array of interactive educational and informational services available to individual Americans via the internet represents an extraordinary resource worth preserving.

- The ideal way to control the flow of information on the internet, and to screen wanted from unwanted information, is not for government to regulate that flow, but rather for each individual user to have the greatest possible control over what they receive.

- The fact that the internet is not centrally controlled and regulated, but largely comprised of content created by millions of individual users, makes it a global forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.

- The internet has flourished, to the benefit of all Americans who rely upon it for a variety of political, educational, cultural, and entertainment services, with a minimum of government regulation.

- Content moderation aimed at keeping websites free from obscenity, stalking, harassment, terrorism, criminal activity, and other objectionable content and behavior should not be penalized by exposing those websites who undertake it to increased liability for their efforts.

Twenty-four years later, while the internet itself has changed in many ways, these fundamental principles remain sound. The task for 21st century lawmakers is to determine whether these goals are being achieved, and to explore ways to address any shortcomings. Remedial legislation, if it is found warranted, should seek to preserve and extend the benefits that Congress overwhelmingly agreed can and should be forthcoming from the internet. Accordingly, any new bill with the goal of updating Section 230 or related areas of federal law should be measured against this template.

In the current Congress, a number of bills have been introduced in both chambers dealing directly or indirectly with content moderation. These include S. 3398, the EARN IT Act; S. 1914, the Ending Support for Internet Censorship Act; H. R. 4027, the Stop the Censorship Act; S. 3983, the Limiting Section 230 Immunity to Good Samaritans Act; and S.4062, Stopping Big Tech's Censorship Act. In this committee, you are considering the Platform Accountability and Consumer Transparency Act (PACT Act), which is aimed at increasing transparency of content moderation policies and ensuring that knowing participation in criminal activity is punishable to the full extent of the law. These are worthy objectives and I commend the committee for prioritizing them.

PACT Act

Considering the PACT Act in light of the original purposes of Section 230, I offer the following observations.

First, the PACT Act itself embraces the important policy objectives set out in the original Section 230. It repeats Section 230's intention to preserve and encourage the continued technological advancement of the internet, in recognition of the substantial benefits the internet provides both to consumers and to the overall economy. The bill also highlights the fact that people throughout the United States rely on the internet for a wide variety of things, including communicating with friends and loved ones as well as the wider world; gathering information from others and broadcasting their own creations; and conducting commercial transactions of endless variety.

Plainly, the purpose of these declarations in the PACT Act is to set out an overarching objective of ensuring that these benefits aren't comprised. This is an aspiration I wholeheartedly endorse. It is also a useful standard against which to measure the operational portions of the bill.

Finally, the preamble to the PACT Act declares that free expression is an essential feature of the internet that should be protected. The bill recognizes that the internet is a uniquely successful facilitator of communications now essential to economic, political, social, and cultural life in America and around the world. This essential characteristic of the internet, which arises from its decentralized architecture that permits millions (indeed billions) of users to interact in real time, was of great importance to me and to the other members of Congress in the mid-1990s when we enacted Section 230. In this respect, the PACT Act and Section 230, at least insofar as their ultimate aims, are aligned.

The bill is divided into three main parts, dealing with transparency, liability, and enforcement. I will address each one in order. Before doing so, I should note several things the bill doesn't do. In each case, in my judgment, the decision of the PACT Act authors to avoid going down these paths reflects the better part of wisdom.

Encryption: The bill eschews the approach of the original version of the EARN IT bill, which had the potential to compromise existing consumer privacy protections by raising the possibility that encryption designed to be secure against everyone except the user who holds the key might expose platforms to new liability. It is a noble legislative aim to incentivize creation of a technically feasible means of "lawful access" that only the government could exploit, but cybersecurity is a constant game of cat-and-mouse in which bad actors are constantly outwitting the latest protections. Despite best efforts, the U.S. government has been hacked many times, and millions of people have lost sensitive information as a result, including not only their Social Security numbers but also detailed private information about their law enforcement, medical, financial, and employment records containing such highly protected data as fingerprints and mental health diagnoses, as well as equally personal information on children and other family members. The Pentagon, the SEC, HHS, the Executive Office of the President, and several member departments and agencies within the intelligence community have been penetrated.

In many cases these successful exploits of U.S. government security have been accomplished by sophisticated foreign actors with state sponsorship.

Congress most certainly should be examining how law enforcement aims can be achieved in tandem with rigorous protection of individual Americans' privacy. But leaping into that morass with mandates or penalties that require the creation of "backdoors," before the technology exists to guarantee that the backdoors will not themselves become the means of illegal exploitation, is premature.

Political Neutrality: As distinct from S.1914 and S. 4062, the PACT Act does not condition Section 230 protections for websites hosting user-created content on their being "politically neutral." Ensuring that the internet remains "a global forum for a true diversity of political discourse" requires that government allow a thousand flowers to bloom—not that a single website has to represent every conceivable point of view. Section 230 does not require political neutrality, and was never intended to do so. Were it otherwise, to use an obvious example, neither the Democratic National Committee nor the Republican National Committee websites would pass a political neutrality test. Government-compelled speech is not the way to ensure diverse viewpoints. Permitting websites to choose their own viewpoints is.

Websites that choose to be politically neutral, and hold themselves out as such, can be held to this standard. When an internet platform promises its customers—through its advertising, published community standards, and terms of service—that its content moderation policy is politically neutral, then that promise can be enforced both by the government and civil litigants under existing federal and state laws. This is far different than a mandate of political neutrality, with the judgment of what is and is not "neutral" placed in the hands of political appointees in Washington. The PACT Act wisely shuns this approach.

Subjective Standards: Several commentators have urged grafting onto Section 230 a requirement, derived from negligence law, upon which existing protections for content moderation would be conditioned. Typically taking the form of a "duty of care" or a "reasonableness" standard, the proposals would effectively make every complaint that a website has failed to meet the standard into a question of fact. Since such fact disputes can only be resolved after evidentiary discovery (depositions of witnesses, written interrogatories, subpoenas of documents, and so forth), no longer could a website prove itself eligible for dismissal of a case at an early stage. An essential feature of Section 230 is its objective standard: was the allegedly illegal material created or developed—in whole or in part—by the website? If the complaint adequately alleges this, then the website can be treated as a publisher and held liable for the material; otherwise not.

Without an objective standard to determine whether lawsuits can proceed, a website would constantly be exposed to open-ended, multi-year litigation over any or all of the user-created content it hosts. The defining characteristic of the internet—the convergence of many (frequently millions and occasionally billions) of users on a single platform—means that a website would have no way to protect itself from a multiplicity of such lawsuits, short of scaling back or eliminating user-created content. Currently, civil suits in the federal system that proceed beyond a motion to dismiss on the pleadings last an average of three years through trial; appeals can consume years more. For this reason, over 90% of cases settle without a judge or jury actually applying the law to the facts in their case. The mere filing of a lawsuit in

such circumstances can create significant settlement value for a plaintiff. The fact that a typical website could easily face hundreds or even thousands of such suits illustrates the severity of the threat to the functioning of the internet itself.

The PACT Act does not seek to graft subjective negligence-type concepts such as a duty of care onto the currently objective criteria in Section 230. Because ensuring that Section 230 can be applied by courts at the motion to dismiss stage is essential to achieving its purposes, this is an important conceptual pitfall for any remedial legislation to avoid.

Monitoring User-Created Content: Essential to the functioning of the internet, and to reaping the benefits of its characteristic feature of real-time communication among unlimited numbers of users, is that websites hosting content do not have to monitor every piece of content. The sheer volume of communications arising from a planetary base of potential users makes this an unreasonable requirement. Even if a website could somehow staff up to meet this near-impossible burden, doing so would ensure that internet communications via that platform could not proceed in real time. Nonetheless, several legislative proposals would impose potential legal liability on websites that could only be avoided by constant monitoring of all user-created content. This is a situation that Section 230 was intended to prevent. The PACT Act wisely avoids the imposition of a monitoring requirement, and indeed contains language in section 5 stating that monitoring or "affirmative fact-seeking" is not required in connection with complaints received. (A similar disclaimer should be added to the bill to clarify that such an obligation does not exist in any case, whether in connection with a complaint or not.)

Takedown Based on Private Accusations: Several commentators have recommended that U.S. law be amended to require, following the model of the Digital Millennium Copyright Act, the mandatory takedown of content once a website has been notified that it is defamatory or otherwise violative of law. Such a requirement would empower anyone willing to allege defamation to require the immediate removal of speech with which they disagree. The PACT Act avoids this pitfall. Instead, its requirement of mandatory takedown of illegal content and conduct applies only when that content or conduct has been determined by a court to be violative of law. While there are other issues created by the language in the bill as drafted, the legislative choice not to create opportunities for the exercise of a "heckler's veto" is the correct one.

Internet Infrastructure Services: Section 230 defines the term "interactive computer service" broadly, because it was intended that the law's protections extend broadly to ensure that content moderation and free expression would be protected. If Congress decides to use Section 230 as a vehicle for placing new burdens and liabilities on web platforms, care should be taken to distinguish between them and the internet infrastructure providers that are swept within the broad definition of "interactive computer service." For example, DNS registries do not operate content publishing platforms and indeed have no direct relationships with end users of the internet. As infrastructure providers, they are very different from social media platforms and search engines. The PACT Act does not attempt to regulate internet infrastructure providers, and indeed the bill includes language forswearing this with respect to web hosting, domain registration, content delivery networks, caching, back-end data storage, and cloud management. This distinction between websites and internet infrastructure providers is an important one to make.

Turning now to the PACT Act's three main sections, and taking them in order, I offer the following comments and suggestions.

Transparency

Transparency—meaning disclosure to consumers, regulators, stakeholders, and the public generally of how a platform moderates content—is a sound objective. The PACT Act's prioritization of transparency is unquestionably constructive and consistent with Section 230 and its ultimate aims.

The mechanisms through which the bill would promote transparency include statutory standards for each website's content moderation policy; mandatory complaint systems for each website that include toll-free call-in services and web-based mechanisms, to be used when websites fail to meet the content moderation standards; required notice and hearing, including a right to appeal, for each complaint received; and mandatory recordkeeping and reporting of content moderation decisions and disposition of complaints. In addition, the Federal Trade Commission is given authority to enforce the statutory standards and the content moderation policies of every website.

While overall these provisions could be made to be workable, as drafted they will run afoul of the objectives of Section 230 and threaten the smooth functioning of the internet and the currently robust environment for user-created content.

'Potentially policy-violating content': Specifically, section 5 of the bill includes in its mandates for an "acceptable use policy" the requirement that websites provide due process notices, hearings, and appeals in response to every complaint that third-party content "potentially" violates the website's community standards. There are three problems with this approach.

First, the website's own standards may or may not be admirable from a public policy perspective. Given that—so long as the statutory requirements concerning illegal content and activity are met—websites are free to adopt whatever content policies they wish, it is reasonable to assume that some websites will welcome content that, while legal, the government would not wish to promote. Any government-mandated complaint system should therefore be focused not on the purely voluntary and idiosyncratic aspects of each website's content policies, but rather on illegal content and illegal activity. This would amply cover not only criminal conduct and content involving sex trafficking, child sexual abuse material, terrorism, illegal drug dealing, stalking, and so forth, but also the wide range of federal and state civil offenses including defamation and invasion of privacy.

Second, the bill's extension of its due process mandate to cover not only *actual* violations of each website's policy, but also *potential* violations, introduces a subjective concept that will be easily abused. Currently, Section 230 permits a court in most cases to judge whether or not the law applies at an early stage, based on the pleadings. This ensures that the mere lodging of a complaint does not trigger elaborate expense for the website—particularly important given the volume of user-created content often handled by even the smallest websites. By reducing what must be alleged in a telephone or email complaint to the mere possibility that content or activity could *potentially* violate the website's policy, the

PACT Act as written would make it trivially easy for anyone to trigger the notice-and-hearing requirements contained in section 5.

Third, the imposition of such a broad notice-and-hearing requirement, which would apply in almost every case given the lax and subjective standard for triggering it, will expose websites to significant expense. (Combined with the high volume of hearings and appeals the bill's subjective standard will generate, its requirement that every complaint be initially researched, analyzed, and disposed of within 14 days will make compliance still more expensive.) Websites will naturally seek to avoid or at least minimize this greater expense.

If almost every complaint requires a hearing and triggers notice requirements and guarantees an appeal, then the only way to minimize the associated expense will be to reduce the grounds for complaints to be filed. Since every website will have control over the specifics of its content moderation policy, the incentive will be to minimize the number of moderation decisions required, through the adoption of less-robust moderation policies. Alternatively, websites could reduce or eliminate user-created content. Section 230, on the other hand, is intended to protect and encourage content moderation, and to facilitate users' ability to publish their content on the internet. In these ways, the inclusion of allegedly "potentially policy-violating content" as a trigger for mandatory hearings and appeals is at odds with the stated goals of Section 230 and the PACT Act itself.

To better align section 5 with the PACT Act's own stated objectives, therefore, it should be amended to eliminate "potentially policy-violating content" wherever it appears. In addition to remedying the problems noted, this would also conform section 5 with the intermediary liability provisions in section 6, which are focused on illegal content and activity, and not on "potentially policy-violating content."

Data collection and reporting: The specific requirements for data collection and quarterly public reporting based thereon, as set forth in section 5 of the bill, include the following:

1. The number of user complaints about specific content
2. The number of employee flags about specific content
3. The number of contractor flags about specific content
4. The number of internal automated flags about specific content
5. The number of government flags about specific content
6. The number of flags about specific content from other service providers
7. The number of flags from outside personnel employed or contracted by other service providers
8. The country of each provider of content that is subject to a complaint or flag
9. The number of times each specific rule within the website's content policy was violated
10. The number of times the website took one of the following actions with respect to content:
    a) content removal
    b) content demonetization
    c) content deprioritization
    d) appending content with an assessment
    e) account suspension
    f) account removal

11. The number of appeals of decisions on complaints about specific content
12. The number of appeals that resulted in restoration of content previously removed
13. Each mechanism used to enforce the website's content policy, including:
    a) Software and hardware tools
    b) General practices
    c) Specific actions
    d) Proprietary techniques[28]

This ongoing data collection burden would be placed on every website in America with an average daily number of visitors of more than 33,333 and $12 million in annual revenue, thereby sweeping in thousands of small businesses that would have to comply.[29] As onerous as the data collection and reporting could be for such websites, the burden would grow exponentially with the size of the platform. The largest social media platforms, Facebook, Twitter, and Yahoo, remove about three billion posts and accounts every 90 days. The number of "deprioritization" decisions, given the daily and even moment-to-moment automated adjustments that would be encompassed within that rubric, would be far higher. The requirement to maintain detailed recordkeeping for all of this for every individual piece of content, which would then become the basis for public reports that would have to be scrubbed for accuracy before publication, would impose a daunting logistical and economic tax on all but the smallest websites.

The disincentives to do content monitoring at all that would accompany these costly impositions would pose a genuine threat to the goals that both Section 230, and ostensibly the PACT Act itself, are aimed at achieving.

Beyond the sheer burden of compliance with this extensive mandate, the language in the bill poses interpretive challenges. None of the terms used in the long list of categories to be tracked is defined. While "content demonetization" has some meaning in common parlance as it relates to Google, for the 875 million other websites in America that is likely not the case. The same can be said for "content deprioritization." Depending upon the website's particular business model, the term might have no application at all; alternatively, each website might be left to define the term for themselves, with endless different variations on the theme. The lack of rigor in drafting this section of the bill would make compliance, already destined to be expensive and burdensome, needlessly more so.

Liability

The PACT Act would amend Section 230 to deny the law's protection to any website that fails to "remove … illegal content or stop illegal activity" within 24 hours of "acquiring … knowledge" of it.

[28] There is an additional requirement that websites report their actions with respect to questionable content, categorized by "coordinated campaign, if applicable." *See* section 5(d)(2)(B)(iv) of the bill. It is not at all clear what this means.

[29] This is a very low threshold. By comparison, the Small Business Association defines a small business as one with less than $35 million in annual revenue. *See* 13 CFR § 121.201. The PACT Act's implicit definition of a "large" business would sweep in websites one-third the size of what the SBA considers to be a small business.

It is clear what is intended here. Conduct and content that are in and of themselves illegal should be kept off of all websites subject to the jurisdiction of the United States. That is an unassailable objective. It is also perfectly consistent with the congressional purposes in enacting Section 230 in the first place. Section 230 was never intended to provide a shield for illegal activity.

Notwithstanding the authors' clear purpose, the actual language in section 6 of the bill creates needless ambiguity that will frustrate achievement of that purpose. Happily, sturdier language in the same section of the bill can be used to clarify some of this unintended ambiguity.

The first drafting problem inheres in the bill's reliance on "knowledge" as the trigger for the 24-hour takedown deadline. "Knowledge" is a subjective standard that requires an assessment of state of mind. "Notice" is an objective standard, which if substituted for "knowledge" in this context would eliminate any subjectivity and at the same time fully achieve the authors' objective. The bill attempts to undo its own use of the subjective term by defining "knowledge" to mean "notice." This creates needless interpretive risk. Since section 6 of the bill already contains a detailed definition of "notice" that amply serves the purpose, all that is needed is to change the proposed amendment to Section 230 to require that the website "has notice of the illegal content or illegal activity, as provided in subparagraph (B)."

The second drafting problem concerns the loose description of what the notice must contain by way of identifying specific illegal content. The bill states only that the notice must contain "information reasonably sufficient" to locate the content. Failing to include specific, clear minimum requirements that will in each case guarantee that the website will be able to locate the offending material virtually guarantees that disputes will arise. Clarity in this respect is particularly important given the very short 24-hour deadline for compliance. (Indeed, as millions of websites are not staffed 24/7 or on weekends, that deadline will in many cases be unrealistic.)

The third drafting problem is the definition of "illegal." The bill defines "illegal" content and activity to be that which a court has "determined to violate Federal law or state defamation law." While tightly circumscribing mandatory takedowns to court-adjudicated cases is a wise legislative choice, more clarity is required here to specify what constitutes a court determination. Must it be a final judgment? Must it await the expiration of appeals? And whichever definition is adopted, what is the rationale? These are questions the bill's authors must directly confront and resolve. From the standpoint of websites that will have to comply with this short-fuse takedown requirement, clarity is more important than the particular answer Congress might settle upon.

From the standpoint of policy makers in Congress, however, which answer you choose is indeed important. Consider that many individuals hostile to others' speech are litigious. The automatic operation of this provision of the PACT Act—mandatory takedown after 24 hours' notice—means that it will be a sure-fire way to suppress speech on the internet. In the case of speech involving important public policy issues, by way of example, should a lower court victory be enough? And what of default judgments, where by definition the arguments on the other side have not been fully considered? What of the deliberate falsification of court orders? (The bill contains no sanction for such activity.) Careful weighing of the tradeoffs here will be necessary to ensure that the objectives of protecting free expression and eliminating illegality from the internet are simultaneously vindicated.

Enforcement

Section 230 was drafted with the intention of protecting the innocent from being held liable for wrongs committed by others. It was equally intended to ensure that those who actually commit wrongs will be subject to prosecution by both civil and criminal law enforcement. One need not rely on the legislative history or the words of the authors for this proposition. The language of the statute is plain enough. If a website, or anyone who provides what the law describes as interactive computer services, is complicit in the creation of unlawful content then it may not claim protection under Section 230. The PACT Act would undo this arrangement. Instead, Section 230 would be waived entirely whenever the federal government or a state attorney general is the litigant. In every such case, websites would lose the protection offered by Section 230.

The only conceivable justification for depriving every website of their existing protection under federal law in this way is that state attorney generals and federal prosecutors are presumed always to be right, and websites in such cases are presumed always to be wrong. If so, one wonders why a trial would ever be necessary. In my experience as head of a federal agency charged with civil law enforcement, the agency was—in the judgment of the courts—more often right than wrong, but hardly infallible. A number of federal departments and agencies in recent years, including the Department of Justice, have been chastised by courts for violating ethical norms in the cases they bring and in the way they have prosecuted them. State attorneys general are all elected political figures involved in political fundraising that frequently presents conflicts of interest. A blanket presumption that the government is always right is too slender a reed on which to rest an across-the-board statutory repeal of Section 230's essential provisions.

There is no reason that federal and state prosecutors cannot enforce all of their laws without need of such a wholesale waiver of Section 230. Indeed, Section 230 itself states that "Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section." So unless flat-out rejection of the very purpose of Section 230 is the objective, the PACT Act should not follow this course. Rather than the blunderbuss approach of simply waiving away the entirety of Section 230 for government litigants, it would be far wiser to more fully accommodate state law enforcement interests through an express statutory authorization to state attorneys general to enforce not only state laws consistent with Section 230, but federal laws as well. This would multiply the potential for enforcement actions to keep illegal content off of the internet.

Such an authorization could be modeled on the existing provision in 28 U.S.C. §543 empowering the Department of Justice to appoint participating state Attorneys General as "Special Attorneys." This authority of the Attorney General to appoint "Special Attorneys" dates to 1966. (The statutory authority was most recently amended in 2010.) The internal Department of Justice authority appears in the United States Attorneys Manual (USAM) at USAM §3-2-200. The authority is very broad, and the terms of the appointment are entirely negotiable. In this way, every state Attorney General who wishes to do so could exercise the full authority not only of his or her state law, but also federal law. As Section 230 has no application to federal criminal law, any theoretical arguments about its application to a given state prosecution will immediately evaporate.

S. 3398, EARN IT

The most recent version of the EARN IT bill was reported from the Senate Judiciary Committee on July 20. As amended in committee, the bill would make several changes to federal law affecting Section 230 and content moderation. The amended bill, like its predecessor, continues to present several serious issues, including constitutional infirmities that could create opportunities for child abusers to escape justice by demanding that the most damning evidence be excluded from their trials.

The bill would mandate the establishment of federal standards, referred to in the bill as "best practices," that would cover, among other things, the following specific ways that websites and internet infrastructure providers should be involved in content moderation. While the bill's focus is content related to child sexual exploitation, the "best practices" would necessarily extend to all content prior to its screening and identification as child sexual exploitation material. The federal standards to be promulgated would include requirements for websites and internet infrastructure providers to:

1. Preserve on their servers specified user-created content
2. Take down specified user-created content
3. Report to law enforcement and others specified user-created content
4. Record and preserve location data for users
5. Record and preserve other personal identifiable information concerning users
6. Develop and maintain an online service for accepting reports from the public concerning specified user-created content
7. Develop and maintain an internal system for sorting, prioritizing, and allocating resources to complaints and reports received through the online public reporting system
8. Implement a "standard rating and categorization system" to identify specified types of user-created content
9. Train content moderators according to the federal standards to be promulgated
10. Provide certain specified levels of support to content moderators devoted to searching for online child sexual exploitation material
11. Produce reports to the government covering:
    a) the entity's policies and procedures for "identifying, categorizing, and reporting" online child sexual exploitation
    b) the entity's efforts "to prevent and disrupt" online child sexual exploitation
12. Coordinate with "voluntary initiatives" related to identifying, categorizing, and reporting specified user-created content
13. Implement "age rating" and "age gating" systems covering all online content
14. Develop "parental control products" to limit the types of websites, social media platforms, and internet content that can be accessed
15. Amend contracts with third parties, contractors, and affiliates to require their compliance with the federal standards
16. Develop internal operational practices operational practices to "ensure" that third parties, contractors, and affiliates comply with the federal standards

This is an elaborate list of both wide-ranging and granular requirements. Yet despite its breadth and granularity, the broad discretion to elaborate upon these themes—which is entirely given over to an ad hoc commission created by the bill—would authorize the promulgation of different or additional requirements that neither Congress nor the regulated community can predict. The specifics of such requirements as the mandatory takedown of user-created content are of enormous importance; yet they are nowhere defined in the bill, and the process for determining them would be wholly within the control of an unaccountable group of political appointees.

The several instances of requiring "searching for" specified user-created content, the requirement to store and preserve it, and the requirement to undertaking affirmative efforts to "prevent and disrupt" users' activity, together amount to a wide-ranging duty to monitor all incoming user-created content. It would otherwise not be possible to find what the websites are instructed look for; necessarily the entire haystack must be searched to find the needle. As protecting websites from having to monitor all user-created content is a fundamental purpose of Section 230, the EARN IT bill fails in this essential respect.

One would hope that, given the deeply intrusive nature of the EARN IT bill's proposed regulation of the businesses of millions of U.S.-based websites, as well as the extension of that regulation beyond websites and consumer-facing internet platforms to a wide variety of internet infrastructure providers, the Congress would be more solicitous of information concerning how its intended new standards would actually operate in the real world. While charging the commission to consider issues of cost and feasibility, there is no check on what the commission can actually prescribe.

Worse, there is no requirement for public input. Ordinarily, when federal agencies promulgate rules, they are first subjected to public notice and opportunity to comment under the Administrative Procedure Act. When commissions are created to advise the executive branch, they are typically subjected to the requirements of the Federal Advisory Committee Act, which similarly ensures public transparency and input. But the EARN IT bill freezes out the public from any right of participation in the process of developing the new federal standards. Instead, a commission comprised of politically-appointed individuals will have free rein to determine what federal "best practices" are, without need of complying with either the APA or FACA. Among other things, this makes it far more likely that whatever standards are promulgated will be uninformed by considerations of how they will, or will not, function in practice.

Were I still a member of Congress, I would insist that, before this legislation proceeds further, it be amended to require the standard public notice and input that is expected for all federal rulemakings.

Beyond the direct impact on websites from the significant compliance burdens that would attend compliance with these elaborate new federal standards, the consequences for every American who uses the internet would be more severe. Whereas today we take for granted the fact that our posts and communications via the internet will be communicated instantaneously, compliance with the new requirements will mean that many user posts will have to be held in suspense, pending review by the website's legal team. Moreover, any user post that create risks to the platform is not likely to survive scrutiny, so that some messages will never be communicated at all. These unintended consequences will mark an unwelcome curtailing of the ease and speed with which Americans share their news and views online today.

Other aspects of the EARN It bill specifically touching upon Section 230 raise different issues.

The amended EARN IT Act carves out a wholesale exception to the law that extends to any claim made in a civil suit under any state law, provided it can be related to child sexual abuse material. The broad scope of the exception—it waives Section 230 state preemption completely—will make it an attractive exploitative opportunity for artful pleading. At a minimum, tightening up the language describing which claims are covered by the exception is required. The language in the PACT Act authorizing enforcement of federal civil laws by state attorneys general is far preferable in this respect. It requires that the underlying claim must also allege a violation of federal law.

An even more serious problem with this across-the-board waiver of Section 230 for all suits based on state laws is that the statutes of several states lack an actual knowledge standard. Instead, they predicate liability on recklessness. As a result, every website would be exposed to new lawsuits alleging that it was reckless in failing to actively monitor all user-created content. It is not difficult to imagine that such lawsuits could be successful. This would effectively impose a nationwide requirement of a duty to monitor—a result that Congress should wish to avoid, and that Section 230 was intended to prevent..

Since not only the new federal standards but also the state-law litigation waived in by the EARN IT bill will strongly encourage monitoring and reporting, there will be new risks of constitutional challenges to criminal prosecutions using evidence reported in this way. Whereas under current law, companies are required only to report known instances of child sexual abuse material, EARN IT constitutes government inducement to actively search for it, and then turn it over for use by the government in prosecutions. This raises the prospect the what are now private searches would be deemed state action, subject to Fourth Amendment scrutiny.

With the exception of the 10th Circuit Court of Appeals (in an opinion written by then-Judge Neil Gorsuch),[30] most courts have held that the mandatory reporting arrangement under current law does not amount to state action, because the actual search that precedes the discovery of the evidence is done voluntarily.[31] But under applicable Supreme Court precedent, private searches are subject to the Fourth Amendment not only when the government requires a search, but when it merely encourages searches. And under the Exclusionary Rule, evidence collected in violation of the Fourth Amendment is generally inadmissible in court.

The risk posed by the EARN IT bill, therefore, is that evidence otherwise available to convict child abusers could now be suppressed.[32]

---

[30] *United States v. Ackerman*, 831 F.3d 1292, 1302 (10th Cir. 2016). *see also, e.g., United States v. Coyne*, 387 F.Supp.3d.

[31] *See, e.g., United States v. Coyne*, 387 F.Supp.3d.387 (2018).

[32] *See* Chris Marchese, *The EARN IT Act's Collision Course With The Fourth Amendment* (2020), https://netchoice.org/wp-content/uploads/2020/06/EARN-It-4A-Report-FINAL.pdf .

A further issue is that the amended EARN IT bill still threatens the privacy protections that websites can extend to their users. While the original version of the EARN IT bill posed a more direct threat to encryption, the amended version continues to give broad authority to its ad hoc commission to promulgate federal standards that would give the government a "back door"—for example, by requiring websites to scan all data before and after encryption[33] or specifying that device manufacturers create custom operating systems allowing government access. (This is not idle speculation: the FBI attempted to convince Apple to do this four years ago.)

Finally, beyond these significant problems, the EARN IT bill's carveout for child sexual abuse material presents the same overall conceptual issue that was present during consideration of FOSTA/SESTA. The sexual exploitation of minors is a serious crime punishable under both federal and state law. But it is one of approximately 4,000 federal crimes and thousands more state law crimes that include terrorism, extortion, mass murder, airline hijacking, rape, hate crimes, hostage taking, sexual battery, torture, and treason. Any one of these crimes can be facilitated using the internet. As with the telephone and the telegraph before it, the internet is frequently a tool of criminals. Section 230, which is designed to apply a uniform federal standard in all civil and criminal cases brought in either state or federal forums, is wholly consistent with the prosecution of criminal and civil claims based on the entire range of illegal activity of which humankind is capable.

It is difficult to argue that, as horrible as the promotion of child pornography is, it is categorically worse than mass murder, terrorism, and a long list of other equally egregious crimes. Nor are these other crimes any less worthy of congressional attention. As Chairman of the House Committee on Homeland Security, I saw firsthand how terrorists use the internet to direct violent extremist acts. Neither in America nor anywhere in the world should terrorists find a "safe space" to operate and disseminate their murderous propaganda of mass destruction. When violent extremists further their plots and grow their ranks by use of the internet, it stands to reason that a nation of laws would not wish to permit laws enacted for another purpose to be used as a shield for such acts. Likewise, when criminal gangs kidnap innocent tourists for exorbitant ransom, using threats of torture and murder, no law should provide them any form of immunity. When assassins target our president, lawmakers, or Supreme Court, no one would want to grant the murderers a legal advantage because they happened to use the internet in the commission of their crimes.

Yet the EARN IT bill would treat these problems categorically differently for legal purposes, providing one set of rules for child sexual abuse material and another, presumably more lenient, set of rules for terrorism.

This represents a fundamental misunderstanding of how Section 230 is intended to operate. It was designed to protect the innocent from being held liable for wrongs committed entirely by others—a principle that should not be waived in any circumstances. It was equally intended to ensure that those who actually commit wrongs will be subject to prosecution by both civil and criminal law enforcement. One need not rely on the legislative history or the words of the authors for this proposition. The language

[33] As one observer has noted, the popular euphemism for this—"client-side scanning"—is what we would otherwise call "reading your messages on your device." Carl Szabo, "The EARN IT Act threatens encryption," *Orange County Register* (July 14, 2020).

of the statute is plain enough. If a website, or anyone who provides what the law describes as interactive computer services, is complicit in the creation of unlawful content then it may not claim protection under Section 230.

Section 230, as written and as interpreted by the courts, is thoroughly consistent with the aggressive prosecution of child sexual exploitation. Equally importantly, it is thoroughly consistent with the aggressive prosecution of all other crimes. It makes little sense to countenance an interpretation of Section 230 that communicates to judges looking at prior decisional law that henceforth, a less stringent rule will be applied in all but the narrow categories carved out of Section 230 by Congress. Each carveout for differential treatment will create significant new legal ambiguities and inexplicable horizontal disparities in both federal and civil litigation. Judges faced with a new Section 230 standard for sex trafficking and child sex abuse cases will be hard pressed not to infer that cases involving other crimes must be decided using a different rule.

It is notable that the most of the nation's attorneys general have written to Congress endorsing a different approach—one that will encompass not only child sexual abuse but all criminal enforcement actions. Such an approach would ensure that courts do not decide to make some internet crimes easier, and some crimes harder, to prosecute. While it would be a mistake to do this by scrapping the uniform federal policy with respect to liability for internet platforms, it is unquestionably correct that uniformity in the application of the federal policy to all crimes is necessary to prevent unintended consequences such as the creation of loopholes that benefit criminals.

Conclusion

I applaud the efforts of Senators on this subcommittee and on the full committee to undertake a thoughtful and dispassionate analysis of the several competing interests involved in keeping the internet free from illegal content and conduct, while at the same time promoting and protecting a vibrant internet ecosystem with the maximum level of free expression. As the co-author of Section 230, which has proven to be a foundational legal underpinning for the internet as it has developed over the last quarter century, I am proud of the role that this law has played in empowering the millions of content creators on the internet, and for the protections it has effectively provided for the freedom of speech of millions of people.

Our reconsideration of the scope of Section 230's protections comes at a time in world history when digital authoritarianism is spreading rapidly around the globe. As Freedom House has noted in its most recent annual report on the state of global internet freedom entitled *Freedom on the Net*, "repressive regimes, elected incumbents with authoritarian ambitions, and unscrupulous partisan operatives have exploited the unregulated spaces of social media platforms, converting them into instruments for political distortion and societal control."[34] They note that while social media in other nations have at times served as a level playing field for civic discussion, they now more often expose citizens to unprecedented invasions of their fundamental freedoms, as governments deploy advanced tools to identify and monitor users on a vast scale. This abuse of social media is occurring not just in well-known cases such as the

[34] *Freedom on the Net 2019: The Crisis of Social Media*, available at https://freedomhouse.org/report/freedom-net/2019/crisis-social-media

People's Republic of China, Russia, Iran, and Saudi Arabia, but also in 38 of the 65 countries covered in their latest report.

America's approach to the regulation of social media, and of speech on the internet more generally, has to date followed a very different model, abjuring government control in favor of private ordering. This has led some critics to argue that private control of the vast amounts of information generated by users of the internet represents a threat to liberty and privacy equal to or greater than would be the result of government control. But two factors militate against this conclusion. Importantly, the private websites and platforms with access to user data are many, and compete with one another. And they lack the powers of a sovereign to aggregate all available data and then to regulate the citizenry through its exploitation. In the hands of government, social media surveillance tools employing artificial intelligence can easily become powerful weapons with which to silence undesirable expression and exert social control.

Before taking even the first baby steps away from the policy Congress and the president endorsed in Section 230 "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation," legislators should be fully aware of where this road could lead.

The landscape of the internet continues to change rapidly, and therefore demands continued vigilant oversight and critical scrutiny by lawmakers. Section 230 is the creation of Congress, and subject to its plenary authority to make and revise laws. It is not written in stone and far from sacrosanct. But it has also provided us with the benefit of a quarter century of practical experience, through continually changing and often challenging circumstances. In the main, it has performed well. To the extent that courts applying it have sometimes given us unwanted results, we can take comfort in the fact that as of 2020 the interpretive kinks that in the past have sometimes let wrongs go without remedy have been for the most part worked out.

Were I still in Congress, though I would be tempted to embellish my original work (like the artist who continues to add a daub here and a brushstroke there, with the result that the painting is never finished), in the current environment I would hesitate to do so. My far greater concern would be the risk, which I have so often seen materialize in the completion of legislation with which I have been involved, that the process of moving the bill through numerous committees, markups, and perhaps an ultimate conference between House and Senate would ultimately run away with my best intentions.

Unlike the placid policymaking environment in which Section 230 was conceived and midwifed into law in 1995-96, today the cacophony that is the debate over social media, content moderation, free speech, and criminality on the internet guarantees not only near-irreconcilable conflicts but also legislative attempts to somehow square the circle. Such deep compromises ranging from the smallest details to high-level issues, which will be necessary if a Republican Senate and Democratic House are to reach any agreement on a bill that achieves their very disparate aims, will likely produce legislation far different from the careful balancing of competing interests that this committee's thoughtful and dispassionate analysis is admittedly capable of producing in the first instance.

In my judgment, the chance that in the end the most important benefits of Section 230 could be undermined, or lost entirely, is a gamble with the future of the internet not worth taking. Recognizing that it is your own judgments on these questions that matter, and that those judgments await your completion of your ongoing analysis of the many issues involved, I stand ready to assist you in any way that I can.

# # # #