ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Proposals to Reform Section 230

ASHLEY JOHNSON AND DANIEL CASTRO I FEBRUARY 2021

In the wide-ranging debate over Section 230, there have been calls to keep the law as it is, repeal it entirely, or reform it. The best approach would be for Congress to pass targeted reforms that address specific harms without unduly burdening online services.

KEY TAKEAWAYS

- Calls for Section 230 reform are growing stronger, but repealing the law is not the answer. Nor is creating significant exceptions that would prevent online services from dismissing costly lawsuits over third-party content.
- Congress should establish a good faith requirement and voluntary safe harbor provisions to protect legitimate online services and prevent bad actors from taking advantage of Section 230.
- Congress also should expand federal criminal law to address forms of harmful online activity that are illegal at the state level, since Section 230 already contains an exemption for federal criminal law.
- The related debate about how to treat political speech online will require solutions outside the scope of reforming or repealing Section 230.

INTRODUCTION

Section 230 of the Communications Decency Act of 1996 is a vitally important law that governs intermediary liability for online services and Internet users in the United States. While the First Amendment gives online services the right to allow or deny lawful speech on their platforms, Section 230 says that these online services are not liable for unlawful third-party content, even when these services make decisions to allow or deny third-party content. This liability protection has had a profound impact on the development of many online services Internet users enjoy daily, including social networks, online retailers, online games, news sites, podcasts, blogs, and more.

Recently, the law has received extraordinary attention from policymakers and pundits, with prominent voices on both sides of the political spectrum blaming the law for a variety of both real and perceived harms on the Internet, including harassment, hate speech, disinformation, violent content, child sexual abuse material, and nonconsensual pornography. Many critics have grown vocal in arguing that the law is broken and are calling for Congress to repeal the law entirely, while others argue that the law should be amended to address concerns its authors could not have envisioned. However, many of the law's proponents say that Section 230 is still appropriate and effective more than two decades after Congress enacted the law, and that attempts to change it, especially repealing it, would come with far-reaching negative consequences.

Section 230 Series

While it is true that many proposals to eliminate or alter Section 230 would undermine online services and pose a major setback to free speech and innovation, that does not mean some targeted reforms are not needed.

Especially in the aftermath of the attack on the U.S. Capitol, criticism of political speech on social media has reached a crescendo. President Trump, along with many of his supporters on the right, have argued that social networks are unfairly removing lawful content, alleging political bias in response to social networks banning accounts linked to far-right groups and conspiracy theories, and labeling some posts as false or misleading. At the same time, President Biden, along with many on the left, have argued that social media companies are too permissive, allowing or even fostering extremist views on their platforms and failing to take sufficient action to moderate harmful political speech. Since the First Amendment prevents policymakers from regulating online speech directly, many have used the threat of Section 230 reform to try to compel social media platforms to either tighten or loosen their content moderation policies. As a result, Section 230 has become a political football; but Section 230 reform is orthogonal at best to address political speech on online platforms.

While it is true that many proposals to eliminate or alter Section 230 would undermine online services and pose a major setback to free speech and innovation, that does not mean some targeted reforms are not needed. Indeed, as this report shows, it is possible to narrow the liability shield to avoid protecting "bad actors" that are not acting in good faith, while also establishing a

voluntary safe harbor provision to minimize nuisance lawsuits and negative spillover effects on innovation. But while reforming Section 230 could address many harms on the Internet, it would not resolve the ongoing debate about political speech, which is grounded more in a debate about the First Amendment and the right set of rules to moderate political speech on large social media platforms than in online intermediary liability. That issue is the subject of a forthcoming Information Technology and Information Foundation (ITIF) report.

This report reviews most of the major proposals for addressing Section 230, including proposals that Congress:

- Preserve Section 230 as it is.
- Repeal Section 230.
- Establish size-based carve-outs.
- Establish carve-outs for certain types of content or activity.
- Require online services to comply with a notice-and-takedown requirement.
- Require "bargaining chips" to receive liability protection.
- Exempt state criminal laws.
- Expand federal criminal laws.
- Expand federal civil enforcement.
- Eliminate the "or otherwise objectionable" clause.
- Establish a "good faith" requirement.

As the report shows, there are a number of options besides keeping Section 230 as it is and repealing it entirely. Each proposed solution has arguments for and against it, but some are more likely to succeed than others.

The report concludes by offering recommendations for how Congress can move forward to address legitimate concerns about Section 230's shortcomings while safeguarding the benefits of the law. To that end, Congress should take the following steps:

- Establish a good faith requirement to prevent bad actors from taking advantage of Section 230(c)(1)'s liability shield.
- Establish a voluntary safe harbor provision to limit financial liability for online services that adhere to standard industry measures for limiting illegal activity.
- Expand federal criminal laws around harmful forms of online activity that are also illegal at the state level.

Notably, as explained later in this report, the establishment of a good faith requirement or a safe harbor provision would be problematic on their own. However, if pursued jointly as part of a Section 230 reform, they would address the weaknesses of implementing either proposal independently.[1]

PRESERVE SECTION 230

One potential solution to the issue of online intermediary liability would be to keep the law in the United States as it is. Many, but not all, proponents of Section 230 argue for this approach on the grounds that Section 230 is responsible for creating many of the best parts of the Internet, and that changes to the law would have serious, and potentially unforeseen, consequences for the online world. Although Section 230 may not be a perfect law, its proponents believe that its myriad benefits outweigh its few flaws.

It is impossible to know exactly how the Internet would have developed without Section 230, but the online world would almost certainly look very different than it does today, likely with less freedom of expression and less of the user-generated content that now forms the backbone of some of the Internet's most visited websites. Indeed, protecting the Internet as it is today is a frequent argument for preserving the liability shield the way it is.[2]

The types of websites and online platforms that benefit from Section 230's liability shield are as diverse as the Internet itself. A lot of the recent controversy surrounding Section 230 primarily focuses on social media giants such as Facebook and Twitter and popular video sharing platforms such as YouTube, but the influence of Section 230 extends much farther. It protects knowledge-sharing websites such as Wikipedia, online marketplaces such as eBay, online classified ads such as Craigslist, countless smaller forums and blogs, and every other website that features product reviews or a comments section, including countless websites of small businesses. It also protects users from liability for forwarding emails or retweeting, thereby facilitating communication between users.

Section 230 protects online services from a wave of lawsuits that could attempt to hold them liable for their users' actions. By allowing these services to thrive, Section 230 forms the foundation of the Internet economy. It has enabled the creation of entire business models that rely on user-generated content.

It is impossible to know exactly how the Internet would have developed without Section 230, but the online world would almost certainly look very different than it does today, likely with less freedom of expression and less user-generated content.

Section 230 makes it easier for smaller online services to compete with larger ones. In a world without Section 230, larger tech companies would have the resources to defend themselves against lawsuits and bulk up their content moderation systems, while smaller online services would not.[3] Smaller online services that rely on user-submitted content—or large-but-less-profitable ones such as Wikipedia, which is run by the nonprofit Wikimedia Foundation—would have to make the difficult decision of whether to continue operating and risk litigation they cannot afford, fundamentally change the services they offer to decrease their risk, or shut down entirely. Such change would further consolidate market share in the hands of a few large online services, giving a boost to some of the social media giants that are the target of much of the anti-Section 230 rhetoric.

Finally, many proposed changes to Section 230 would have serious implications for the freedom of speech online. Without Section 230 guaranteeing that they will not face liability for third-party content on their platforms, online services would have strong incentives to take a more restrictive

approach to content moderation. Instead of just removing content that clearly violates the law or their terms of service, they would also likely remove any content that falls into a gray area where it may or may not be objectionable, because to not do so would mean risking legal trouble. This is known as "collateral censorship," a form of self-censorship that occurs "when *A* censors *B* out of fear that the government will hold *A* liable for the effects of *B*'s speech."[4] For example, platforms may choose to remove lawful, but controversial, political speech—exactly the type of speech the First Amendment was designed to protect—in order to avoid expensive nuisance lawsuits from those who claim to find that political speech objectionable.

Any changes to Section 230 will have far-reaching consequences, but given the current controversy surrounding the law, doing nothing is increasingly not a politically feasible option. The calls for reform are part of a larger trend of public backlash against Big Tech—or "techlash"—that do not appear to be going away any time soon. If Section 230's supporters refuse to budge from their stance that Section 230 should remain exactly the way it is, they will effectively hand the reins over to the law's detractors to craft a new intermediary liability law that may go too far in the other direction. Instead, to address legitimate concerns about stopping bad actors, supporters should offer solutions that still protect freedom of expression and innovation.

REPEAL SECTION 230

Some of Section 230's critics want to repeal the law altogether and leave the issue of online intermediary liability to the courts. They argue that the law does more harm than good, unfairly protecting bad actors, enabling various forms of illegal or harmful online content, immunizing providers from liability for unfairly removing users and content, and giving online services a free pass that no other type of business enjoys. For example, Rep. Louie Gohmert (R-TX) introduced H.R. 8896, the Abandoning Online Censorship Act, to repeal Section 230.[5]

The first argument, that Section 230 protects websites that host illegal content, is a common one. Critics frequently refer to the so-called bad actors that hide behind 230's liability shield. Before Congress passed the Allow States and Victims to Fight Online Sex Trafficking Act and the Stop Enabling Sex Traffickers Act (FOSTA-SESTA) in 2018, adding an exception to Section 230 so that it would no longer apply to sex trafficking, critics frequently cited Backpage as an example of a bad actor.

But sites such as Backpage are not the only bad actors online. There are untold numbers of online services whose users post child sexual abuse material, nonconsensual pornography, defamatory "gossip," terrorist communication, and more. While some of this illicit content slips through the cracks of the content moderation systems of legitimate platforms, other platforms do little to stop it. By immunizing platforms against civil liability for third-party content, critics argue, Section 230 prevents the victims of these crimes from seeking justice against the online services that possibly could have prevented others from sharing this content.

In addition to hosting illegal content, some online services are a source of legal but harmful forms of online abuse, including hate speech and harassment. Online abuse can lead victims to delete their social media profiles, shut down their websites and blogs, and in extreme cases when online abuse trickles into the physical world, move and change their name or engage in self-harm.[6] Because online abuse disproportionately affects marginalized populations, this is detrimental to equal protection.[7] Again, because of Section 230, victims cannot sue social media platforms for failing to act against hate speech and harassment posted by their users.

Some conservative policymakers, including former President Trump, call for repealing Section 230. They believe it is unfair for large social media platforms to benefit from Section 230's liability shield when, in their view, these sites are biased against conservative viewpoints, blocking or suspending accounts from conservatives and removing posts that express conservative political opinions. There is no evidence of systemic conservative bias, and the First Amendment protects the free speech rights of these platforms to make decisions about what content and which users they allow on their platforms.[8] However, Section 230(c)(2) protects these companies from liability for removing content they believe to be objectionable.[9] Eliminating Section 230 would expose these companies to nuisance lawsuits.

Some liberal policymakers, including President Biden, have called for repealing Section 230, but for the opposite reason. They believe that it is unfair for large social media platforms to benefit from Section 230's liability shield when users spread hate speech, misinformation, and other objectionable content on their platforms. However, repealing Section 230 would negatively impact the free speech of marginalized populations that these policymakers are often trying to protect. Online services would be disinclined to host content relating to controversial political movements such as #MeToo or Black Lives Matter if individuals and groups who opposed those movements, including the targets of their activism, could sue the online services that hosted their discussions and facilitated their organization.

The legal landscape prior to Section 230 reveals how repealing the law would be detrimental.

Finally, some critics argue that Section 230 treats online services differently from other businesses. If a physical business facilitated child exploitation or terrorist communication, or if a traditional publication printed user-submitted nonconsensual pornography or defamatory statements, they likely would not escape civil liability. Why, they ask, is the law different for online services, especially since many websites profit from user-submitted content, including illegal content? Critics argue that if moderating that content proves difficult, online services should solve the problem or design their services in a less negligent way to prevent these problems from occurring in the first place.[10]

But the legal landscape prior to Section 230's passage reveals how repealing the law would be detrimental. Section 230 arose out of a pair of court cases in the 1990s: *Cubby v. CompuServe* (1991) and *Stratton Oakmont v. Prodigy* (1995).[11] Taken together, these cases established a counterintuitive precedent for websites that rely on user-generated content: Websites that exercised no control over what was posted on their platforms and allowed all content would not be liable for user content, while websites that exercised good faith efforts to moderate content would face liability. This is the legal landscape America would return to if Congress repealed Section 230.

Some critics argue for repealing Section 230 and also overturning the *Cubby* and *Stratton Oakmont* cases that made online services that moderate content liable for their users' speech, so online services would still have an incentive to moderate content. But even without that legal precedent, repealing Section 230 would still have negative consequences for innovation, free speech, and competition. Large online services would adapt to a world without Section 230, while smaller ones may not have the resources, which would only further consolidate the market

share of large platforms. Moreover, platforms would turn to overly cautious and restrictive content moderation practices, removing any potentially objectionable content, which may include valuable forms of expression such as political speech and marginalized speech.

ESTABLISH SIZE-BASED CARVE-OUTS

One proposal to reform Section 230 would introduce size-based carve-outs for intermediary liability so that only large online services would lose Section 230 protection. In other words, Section 230 would only apply to smaller companies, not large ones. The purpose would be to safeguard competition from smaller online services that would not survive without Section 230 protections. This type of proposal is also a manifestation of the ongoing techlash, as it aims to create stricter rules for tech giants for their perceived content moderation failures.[12]

The problem with Section 230, these critics argue, is that the law says online services that host third-party content "shall not be treated as the publisher or speaker" of that content. But large social media platforms are like publishers in two important ways.[13]

First, large social media platforms actively moderate content, deciding what content appears on their platforms and what is taken down. This is not too different from how some early forums and online bulletin boards operated. The difference, critics claim, is that large social media platforms such as Facebook and Twitter are far more ubiquitous than their 1990s counterparts, and their content moderation decisions impact hundreds of millions or even billions of users.[14]

Second, social media platforms amplify content, running algorithms that determine who sees what, and sometimes these algorithms promote harmful content.[15] Critics argue that when large platforms amplify harmful content, the impact is so significant (because hundreds of millions of users may see it), they should be liable for this content.[16]

The first problem with size-based carve-outs is, counterintuitively, they would actually be detrimental to competition. A small online company would benefit from Section 230 immunity, which would hopefully enable it to succeed and grow. But as it grew and approached the threshold at which it would lose immunity, it would have to make a difficult decision: pass the threshold and adapt on its own to a difficult new set of rules, or get acquired by a larger company that has already established its ability to succeed without immunity. Acquisition by a large, successful company is already a tempting offer; size-based carve-outs would further incentivize small companies to get acquired instead of continuing to grow on their own.[17]

Additionally, virtually all the "bad actors" critics reference when debating Section 230 are smaller companies. Large, established online services such as Facebook, Twitter, and Google have many incentives to address illegal and harmful content on their platforms, not the least of which being their reliance on advertising revenue. Most advertisers, especially national brands, do not want to be associated with websites known for hosting illegal activities or abuse. But there are smaller online services that profit directly from illegal or abusive third-party content—revenge-porn websites, for example—and under a size-based carve-out, they would continue to benefit from Section 230 immunity while many legitimate larger online services would not.

Finally, even if only large platforms had to do without Section 230, collateral censorship would still pose a problem. Smaller websites would have more freedom in their content moderation practices, but larger websites—the websites billions of people use daily around the world—would

be more restrictive about the types of content they allow, thereby limiting free expression online. In addition, to the extent this allows smaller, more niche online services to thrive, it could further drive political polarization as people flock to like-minded online communities.

ESTABLISH CARVE-OUTS FOR CERTAIN TYPES OF CONTENT OR ACTIVITY

Similar to the proposal to keep Section 230 as is but create an exception for online services of a certain size, another proposal would keep Section 230 as is but create an exception for certain types of content or activity. These proposals usually target a specific form of illegal content or activity that is particularly harmful, such as sex trafficking, and would prevent online services from taking advantage of Section 230's liability shield if they fail to remove this content or activity when they become aware of its existence on their platform.

The Allow States and Victims to Fight Online Sex Trafficking Act and the Stop Enabling Sex Traffickers Act (FOSTA-SESTA) is the most prominent example of a carve-out for a certain type of content or activity. Congress passed the amendment in 2018 in response to alleged sex trafficking taking place on classified advertising websites, particularly Backpage.[18] The amendment created an exception to Section 230's liability shield for sex trafficking. Section 230 has always contained an exception for federal criminal law, so online services could still face federal criminal liability for facilitating sex trafficking, but after FOSTA-SESTA, online services can also face federal and state civil liability.[19]

Sen. Mark Warner (D-VA) introduced the Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms (SAFE TECH) Act, which would add several exceptions to Section 230's liability shield. Under the SAFE TECH Act, Section 230 would no longer apply to ads or paid content, civil rights law, stalking or harassment laws, wrongful death actions, or human rights violations abroad. Section 230 would also no longer apply when an online service fails to remove content upon receiving a court order.[20]

The risk of carving out certain types of content or activity from Section 230 is it requires online services to determine what is legal or illegal, which can lead to over-enforcement. In order to avoid liability, online services may remove forms of content that fall within a gray area. In the example of FOSTA-SESTA, many online services shut down their classified advertising or dating services that could be used to facilitate sex trafficking but were not designed to do so. Some messaging and cloud storage services also removed any adult content their users shared or stored, even if the content was legal.[21]

In addition, multiple carve-outs to Section 230's liability shield would render the shield virtually useless. There are many forms of illegal content and activity online the government, most Internet users, and most online services would all agree are harmful: terrorist content, child sexual abuse material, drug trafficking, nonconsensual pornography, and more. But adding exceptions for all these illegal activities would subject online services to numerous lawsuits that Section 230 was designed to protect them against. This would impact not just bad actors that knowingly profit from illegal content, but also legitimate online services that make good faith efforts to keep illegal content off their platforms.

REQUIRE NOTICE AND TAKEDOWN

There are various proposals to make Section 230's liability protections conditional on online services meeting certain conditions. One proposal is a notice and takedown requirement, which

would require online services to remove illegal content—but not necessarily content that is harmful but still legal—in a certain amount of time, or face penalties. This proposal borrows ideas from the United States' approach to online copyright infringement, as well as some other countries' approaches to intermediary liability. Under a notice-and-takedown approach, websites would receive liability protection for third-party content if, upon receiving a notice that the content is unlawful, they followed a set of procedures for removing it. If they failed to do so, they could be liable for the content.

Passed in 1998, the Digital Millennium Copyright Act (DMCA) established a notice-and-takedown process for addressing online copyright infringement. Under the DMCA, copyright owners can alert an online service to infringing third-party content on their platform by sending them a notice. In response to a valid notice, the service must remove the infringing content "expeditiously" in order to avoid liability. The individual who posted the content may submit a counter-notice if they believe the notice was mistaken and the content is not infringing. If the individual who filed the original notice does not take any further action within 10 days, the service must then restore access to the content.[22] A notice-and-takedown approach to intermediary liability could follow a similar process, replacing "infringing content" with "unlawful content." Countries that have a notice-and-takedown approach to intermediary liability include New Zealand (Harmful Digital Communications Act 2015), South Africa (Electronic Communications and Transactions Act, 2002), and the United Kingdom (Defamation Act 2013).

Sen. Brian Schatz (D-HI) introduced S. 4066, the Platform Accountability and Consumer Transparency (PACT) Act, which includes a notice and takedown provision for intermediary liability. If an online service is notified of illegal content or activity on its platform and fails to remove the content or stop the activity within 24 hours, it could be liable for that content or activity.[23]

The notice-and-takedown approach has a number of shortcomings. First, online services would struggle with responding to invalid and incomplete notices. This problem exists under the DMCA, where online services occasionally receive notices from copyright holders against content that is lawful under fair use or that do not comply with the requirements for a valid notice.[24] Making these determinations can be difficult with regards to copyright infringement and would be even more difficult for other forms of potentially unlawful speech. In addition, requiring online services to remove unlawful content would do nothing about the forms of content that are harmful but legal, including hate speech, misinformation, and bullying, a key concern for many policymakers, especially on the left.

Another problem is online platforms struggle with keeping content off their platforms that they have already removed once. Users may repost the prohibited material from a new account, or they may slightly alter the content, which would require reviewing the content again. With regards to copyright, it is possible to implement a "notice-and-stay-down" policy, wherein online services use automated tools to review subsequent uploads against known infringing material. But implementing such a policy for text messages would be much more difficult, if not impossible, because of the difficulty of building systems that can automatically recognize nuances in language. Notice and takedown effectively creates a "Whac-A-Mole" problem which online services would likely struggle to keep up with.[25]

Sen. Warner (D-VA) has proposed establishing a process whereby victims of deepfakes—realistic-looking images and videos produced with artificial intelligence that portray someone doing or saying something that never actually happened—who obtain a judgment against an individual who created offending content could then give notice of this judgment to online services. Online services would then be liable under state tort law if they failed to take down the content or prevent it from being re-uploaded in the future.[26] However, there are a number of limitations to this proposal. First, this would only deal with deepfakes, and only in cases where state law provided protection for individuals. Second, obtaining a judgment against an individual may prove difficult for victims of defamatory deepfakes, especially if they are unable to identify the creator. Finally, this proposal would help individuals remove this content from some large platforms, but they would likely struggle to identify all the potential sites where someone could upload this content.

USE LIABILITY PROTECTION AS A BARGAINING CHIP

Policymakers have advanced various "bargaining chip" proposals that would extend Section 230 liability protections to online services only if they made certain concessions—ranging from a potential ban on end-to-end encryption to adopting terms of service that prohibit users from posting hateful content to eliminating the use of algorithms to rank content in social media news feeds and targeted advertising based on users' preferences and behavior. Policymakers have proposed varying requirements, but all are generally meant to establish certain minimum guidelines online services would have to implement to keep illegal and objectionable content off their platforms in order to receive liability protection. Any platforms that do not follow these rules—generally thought to be the bad actors—would not benefit from Section 230's liability shield.

For example, former Representative Beto O'Rourke, in addition to calling for a notice-and-takedown provision in Section 230, proposed changing the law to require "large internet platforms to adopt terms of service to ban hateful activities" which would include "those that incite or engage in violence, intimidation, harassment, threats, or defamation targeting an individual or group based on their actual or perceived race, color, religion, national origin, ethnicity, immigration status, gender, gender identity, sexual orientation or disability."[27] The goal of his proposal is to limit hate speech and the violence that results from it—such as that which came in the wake of a white supremacist shooting in El Paso, Texas.

There are three primary problems with this proposal. First, its impact is unlikely to have a significant impact because all the major social media platforms already including these types of requirements prohibiting hate speech. Second, any attempt by Congress to limit legal speech, which can include some forms of hate speech, would likely encounter First Amendment challenges. And finally, if social media platforms more aggressively enforce content moderation policies against offensive speech, they may face even more political backlash since policymakers across the political spectrum often disagree on what content should be removed or remain online. With red and blue America engaged in an increasingly hot culture war, it is difficult to imagine there will be consensus any time soon on where the boundaries should be.

As another example of a bargaining chip proposal, Sen. Josh Hawley (R-MO) introduced S. 1914, the Ending Support for Internet Censorship Act, which would require companies with over 30 million active monthly users in the United States, over 300 million worldwide active monthly

users, or more than $500 million in global annual revenue to prove to the Federal Trade Commission every two years that their algorithms and content moderation practices are politically neutral in order to receive Section 230 liability protection. This proposal hearkens back to the Federal Communications Commission's (FCC) "fairness doctrine," which required broadcasters to present news with a balanced perspective, although the FCC abolished the fairness doctrine in 1987.[28] This proposal is one of the clearest examples of how policymakers are using Section 230 as a way to force social media platforms to adjust their content moderation policies. Notably, the proposal would not change any of the core principles of Section 230, and would only extend protections to large social media platforms only if they agree to be politically neutral, which is a characteristic that is difficult to measure.

Sen. Schatz's PACT Act also includes bargaining chip elements, requiring online services to enact certain transparency measures and provide a complaint system for users to report content that is illegal or violates the platforms' policies and appeal platform decisions to remove user-submitted content in order to continue benefiting from Section 230's liability protections.[29]

Other bargaining chip proposals include H.R. 492, the Biased Algorithm Deterrence Act of 2019, introduced by Rep. Gohmert, which would eliminate Section 230 protections for any social media service that did not remove all technical measures that filter or sort user-generated content.[30] This bill would require social media sites to display all content in chronological order to receive liability protection for third-party content. Similarly, H.R. 8515, the Don't Push My Buttons Act, introduced by Rep. Paul Gosar (R-AZ), would eliminate Section 230 protections for online services that curate the content users see based on personal data without their affirmative consent.[31] This would, however, negatively impact many of the features social media platforms offer, such as news feeds that sort stories according to what is most likely to interest users, and features that allow users to explore or discover new content that is similar to content they have liked or interacted with in the past. These features add immense value to users, whereas simply displaying content in chronological order would force users to scroll through content that does not interest them.

There are also multiple bargaining chip proposals that target online services that rely on advertising as a source of revenue. H.R. 8922, the Break Up Big Tech Act of 2020, introduced by Rep. Tulsi Gabbard (D-HI-2), would eliminate Section 230 protections for online services that sell advertisements that are displayed to users based on their preferences and behavior. It also contains similar provisions to the Biased Algorithm Deterrence Act and Don't Push My Buttons Act that would treat online services as publishers if they display content in any order other than chronological.[32] Finally, S.4337, the Behavioral Advertising Decisions Are Downgrading Services (BAD ADS) Act, introduced by Sen. Hawley, would eliminate Section 230 protections for any online service that engages in behavioral advertising. These proposals targeting behavioral advertising fail to acknowledge the benefits of displaying ads according to users' preferences. Not only is selling targeted ads an important source of revenue for many online services, enabling them to offer their services to users for free and to continue offering new features and innovations to the site, it also results in users seeing ads for products and services that are more likely to interest them.

Finally, Senator Lindsey Graham (R-SC) introduced a bargaining chip proposal with S. 3398, the Eliminate Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act.[33] The bill

would establish a National Commission on Online Child Sexual Exploitation Prevention that would draw up a series of best practices for services to prevent online child sexual exploitation. If online services failed to follow those best practices, they would lose Section 230 protection from claims related to child sexual exploitation laws.

The original bill, introduced in March 2020, would have given the U.S. attorney general the power to add to the list of best practices services must follow in order to retain Section 230 immunity. Given that the attorney general at the time, William Barr, had a firm stance on end-to-end encryption, many tech companies and privacy and security advocates worried that he would use it as an opportunity to declare that companies that use end-to-end encryption are not following best practices to prevent child exploitation. The fact that Sen. Graham had also spoken out against end-to-end encryption increased suspicion surrounding Barr's motivations.[34]

The EARN IT Act is a prime example of a problem with bargaining chip proposals: They are an easy way for lawmakers to pursue a secondary agenda under the guise of curtailing online crime and abuse. If Congress decides to amend Section 230 or replace it with another piece of legislation, it will need to focus solely on the issue at hand: intermediary liability. Bargaining chip proposals allow Congress to use intermediary liability legislation as a mechanism to settle unrelated issues, which it should instead resolve with separate legislation that specifically addresses those issues.

EXEMPT STATE CRIMINAL LAW

Another proposal to reforming Section 230 is to add an exemption for state criminal law. There are already a few exceptions to Section 230's liability protections; namely, it does not apply to federal criminal and intellectual property law or to sex trafficking law.[35] Some critics, in particular a number of state attorneys general, argue that adding an exception for state criminal law would help curtail forms of online abuse that are only illegal at a state level.[36]

This reform would be a relatively small change, and would only require adding a few words to Section 230(e)(1), where it currently reads that "nothing in this section shall be construed to impair the enforcement of … any other Federal criminal statute," and would instead state that "nothing in this section shall be construed to impair the enforcement of … any other Federal, State or Territorial criminal statute."[37]

Proponents of this solution, which include attorneys general from the other 47 states and territories, argue that in the United States, state and federal laws complement each other.[38] The federal government is best equipped to handle some issues, but other issues are better left to the states, just as federalism intended. But critics argue this system does not work when laws such as Section 230 preempt certain state laws and create a gap in enforcement. A popular example of this gap is nonconsensual pornography, as there is currently no federal law criminalizing "revenge porn"—only state laws.[39] Since Section 230 does not apply to state criminal laws, victims cannot pursue legal recourse against revenge porn websites, only against the individuals who initially shared their information. But states also point to other issues, such as deepfakes, for which there are not federal laws; or problems such as identity theft and black-market opioid sales, wherein states play a significant rule in enforcing these laws.

There are some problems with this proposal. First, most crimes are already covered by federal law. Revenge porn is a notable exception, but it is one of the few. To the extent that there are

gaps, Congress should pass federal laws to cover these areas. Second, online services would have to keep up with a patchwork of 50 different sets of state criminal laws instead of a single set of federal laws, which would be a more difficult task—although it is one that many large companies already have to contend with. Finally, with 50 different states to contend with, as well as 50 different attorneys general, the chances are much higher that one or more of them will pass a bad law that is overly burdensome on online services or takes unexpected enforcement action against an online service. Allowing states to set their own rules for online intermediary liability would allow any one state to effectively set national policy. For example, a state could make online services criminally liable for any illegal activities by users on their platforms when they have "actual knowledge" of such activity—a liability standard that has been rejected at the federal level because of the negative impact it has on services that may seek to moderate their platforms less rigorously in order to avoid liability, to the detriment of their users.

EXPAND FEDERAL CRIMINAL LAWS

As an alternative to adding an exemption to Section 230 for state criminal law, Congress could expand federal criminal law to cover a wider range of illegal activity. Most online crimes are already covered by federal law, including identity theft, child pornography, cyber extortion, hacking, trafficking passwords, and online solicitation of a minor.[40] However, there are certain activities some states have outlawed but the federal government has not, including deepfakes, cyberbullying, and nonconsensual pornography. The federal government could pass laws not only around deepfakes, cyberbullying, and nonconsensual pornography, but also around foreign interference and propaganda in U.S. elections.

Expanding federal criminal law to include these activities would carry fewer negative consequences than alternative approaches: namely, adding an exception to Section 230's liability protections for specific types of content or activity or adding an exception for state criminal law. Congress did the former when it passed FOSTA-SESTA in 2018, opening online services up to civil liability and state criminal liability for violating sex trafficking laws. As a result, Craigslist shuttered its Personals section and other websites similarly stopped offering certain services simply because those services could be misused and the websites themselves did not want to face liability for that potential misuse.[41]

As opposed to these proposals that attempt to solve the issue of certain illegal activity by creating additional exemptions to Section 230, expanding federal criminal law would address the issue by taking advantage of the existing exemption in Section 230 for federal criminal law. It would also avoid creating a patchwork of inconsistent state laws and enforcement for online services—which almost always have users in multiple states—to contend with. Finally, expanding federal criminal law would not open online services up to civil lawsuits that would carry high legal expenses.

Expanding federal criminal law would allow the federal government to prosecute online services that engaged in illegal activity—such as soliciting revenge porn—but would not hold online services accountable for the actions of criminals who misused their platforms. The latter would place an unreasonable burden on online services and perhaps even incentivize them to monitor their users' behavior for criminal activity, a potential privacy violation.

EXEMPT FEDERAL CIVIL ENFORCEMENT

The Department of Justice (DOJ) released its reform proposal for Section 230 in September 2020. As part of this proposal, DOJ suggested amending Section 230 to make it clear that the law's liability shield does not apply to federal civil enforcement. This would function similarly to the exemption that already exists in Section 230 for federal criminal prosecution, allowing the U.S. federal government to go after online services that have broken federal law in both criminal and civil court.[42]

Specifically, DOJ's proposed exemption would apply to civil action by the federal government against an online service "related to a specific instance of material or activity that, if knowingly disseminated or engaged in, would violate federal criminal law," as long as the service had "actual notice" of the material or activity's existence and unlawfulness and failed to remove it, report it to law enforcement where required by law, or preserve evidence of it. In such a case, an online service could not use Section 230(c)(1) as a defense against the federal government in civil court, just as it cannot use Section 230(c)(1) as a defense against the federal government in criminal court.[43]

DOJ's argument is that federal civil enforcement complements federal criminal prosecution. In addition, its proposal to exempt federal civil enforcement is a compromise between the current law, which preempts all civil cases against online services related to third-party content (other than those already exempted by FOSTA-SESTA) and proposals that would allow private citizens to sue online services for failing to remove harmful or illegal third-party content. The latter would subject online services to countless nuisance lawsuits, while the DOJ's proposal would only subject services to civil action from the federal government.

However, it is unclear exactly when such federal civil enforcement would be necessary. If an online service is contributing to illegal activity, such as was alleged with Backpage, then DOJ can bring criminal action against them. Enforcement agencies such as the FTC wanting to bring cases against online intermediaries, but lacking statutory authority, should be considered separately from Section 230 reform.

ELIMINATE THE "OR OTHERWISE OBJECTIONABLE" CLAUSE

Another reform proposal focuses on narrowing the scope of Section 230(c)(2), which states that online providers shall not be held liable for actions taken in good faith to remove harmful third-party content. Specifically, this section affirms that providers and users are not liable for limiting access to "material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."[44] In particular, critics point to the "or otherwise objectionable" phrase as being too open-ended. Rep. Gosar introduced H.R. 4027, the Stop the Censorship Act, which would strike this entire lengthy clause and replace it with the phrase "unlawful material."[45]

Two Senate bills, S. 4534, the Online Freedom and Viewpoint Diversity Act, and S. 4632, the Online Content Policy Modernization Act, introduced by Sen. Roger Wicker (R-MS) and Sen. Graham, respectively, would similarly change the language of Section 230(c)(2). Both bills contain a provision that would replace the "otherwise objectionable" phrase with the more-specific "promoting self-harm, promoting terrorism, or unlawful." The bills would also raise the

standard for Section 230(c)(2)'s liability shield, which currently protects online services from liability for removing content they consider to meet that criteria, by instead only protecting them from liability for removing content they "have an objectively reasonable belief" meets the criteria.[46]

These proposals arose from allegations that major online platforms discriminate against and censor conservative speech. These claims have gained even more support in some circles after Facebook, Twitter, Instagram, and other platforms banned or suspended President Trump after rioters broke into the U.S. Capitol on January 6, 2021.[47] But restricting the types of content online services can remove without potentially facing liability would come with serious adverse side effects.

One of Congress's primary intentions in passing Section 230 was to encourage good faith content moderation. To achieve this, Section 230 gives online services the freedom to moderate content in a way that best suits their users. This freedom has allowed for the development of many different types of online platforms, each experimenting with moderation policies that work best for their communities. Indeed, there is no one-size-fits-all set of content moderation policies that is appropriate for every platform, and platforms regularly update their content moderation policies based on user feedback. If enough users are dissatisfied with an online service's content moderation, they can create demand for a new, competing service. Tightening the standard for Section 230(c)(2) would incentivize less content moderation, especially of content such as misinformation and bullying that falls into the gray area of being harmful but not illegal.[48]

ESTABLISH A GOOD FAITH REQUIREMENT

Another proposed reform to Section 230 would be to add a good faith requirement to Section 230(c)(1). This would address the problem of bad actors—websites that knowingly host and profit from illegal or harmful material—taking advantage of Section 230 immunity. It would borrow from Section 230(c)(2), which already contains a "good faith" requirement.

Section 230(c)(2) states that online service providers are not liable for "any action voluntarily taken in good faith to restrict access to or availability of" objectionable content.[49] It applies to content that providers remove, and gives providers leeway in their content moderation decisions, as long as they act "in good faith." A specific case of a provider not acting in good faith when removing content occurred in *E-Ventures Worldwide v. Google* (2016), when Google was found to have acted anticompetitively in removing E-Ventures' listings on its search engine.[50]

Section 230(c)(1), however, applies to all content that providers do not remove, and does not contain a good faith requirement. Adding such a requirement would allow legitimate websites to continue benefiting from Section 230 protection, without shielding bad or negligent actors. Ideally, this language would be as simple as exists in 230(c)(2), leaving the interpretation of what constitutes acting in good faith to the courts. However, this should not include online services that act negligently, allowing illegal or harmful content to proliferate; purposefully profit from illegal or harmful content; or design their services in order to encourage illegal or harmful content.

A similar proposal comes from Danielle Citron and Benjamin Wittes, who proposed modifying Section 230(c)(1) to state that it only applies to a provider that "takes reasonable steps to prevent or address unlawful uses of its services."[51] The idea of this proposal is also to eliminate

immunity for bad actors. As with adding a good faith provision, this would allow providers to maintain broad liability protections provided they can prove to a court that their response is reasonable.

Sen. Hawley introduced S. 3983, Limiting Section 230 Immunity to Good Samaritans Act, which would require online services to add a good faith standard to their terms of service, with a fine of at least $5,000 for violating that standard. The bill has a size-based carve-out and would apply only to online services with over 30 million U.S. users, 300 million global users, and $1.5 billion in global revenue over a 12-month period. The bill also allows users to sue online services for violating the good faith standard in their terms of service. The bill's definition of an online service not acting in good faith includes selectively enforcing the terms of service, failing to honor a public or private promise, or any other action taken with "fraudulent intent."[52]

There are two main risks of a good faith requirement. First, courts may not take sufficient action against bad actors. Ideally, the Congressional Record, however, would make clear what types of bad actors Congress had in mind when it discussed online services that do not act in good faith. Second, a good faith requirement would make it significantly more difficult for online services to defend themselves against nuisance lawsuits, as not only would they have to prove that they are immune from liability under Section 230 for third-party content, but they would have to satisfy the greater burden of proving that they have acted in good faith, which would likely open up much more costly litigation.

Table 1: Impact of various Section 230 proposals

Proposal	Impact on Nuisance Lawsuits	Impact on Protected Speech	Impact on Innovation	Impact on Illegal Activity	Impact on Harmful, but Legal, Activity
Do Nothing	Online services and users are protected against lawsuits related to third-party content	Online services can determine what content is permitted without risk from frivolous lawsuits	Organizations can build services and businesses models based on user-generated content	Federal criminal law applies but online services are not subject to state criminal law and have no civil liability for illegal activity of their users	Market forces incentivize some online services to curtail harmful activity, but some bad actors may also benefit from immunity
Repeal Section 230	Online services and users have no protection against lawsuits related to third-party content	Online services have an incentive to censor controversial speech to avoid liability	Higher legal costs raise the barrier to entry for new online services	Online services must remove illegal content or face criminal and civil liability	Online services must remove harmful content or face civil liability
Establish Size-Based Carve-Outs	Smaller online services are protected against lawsuits related to third-party content, but large services have no protection	Large online services have an incentive to censor controversial speech	Incentivizes growing online services to get acquired	Illegal activity could continue on small online services	Harmful activity could continue on small online services
Establish Carve-Outs for Certain Types of Content or Activity	Online services are protected against lawsuits, except those relating to specific forms of illegal third-party content	Online services have an incentive to remove content that falls into a legal gray area	Online services may disable features or services that could expose them to liability	Online services must remove certain forms of illegal third-party content	Does not target harmful, but legal, activity

Proposal	Impact on Nuisance Lawsuits	Impact on Protected Speech	Impact on Innovation	Impact on Illegal Activity	Impact on Harmful, but Legal, Activity
Bargaining Chip Proposals	Online services are protected against lawsuits related to third-party content if they meet certain requirements	Depends on the type of activity the proposal targets	Depends on the type of activity the proposal targets (e.g., some target technologies such as encryption)	Only targets a specific type of illegal activity (e.g., CSAM, terrorism, cyber-stalking)	Does not target harmful, but legal, activity
Notice and Takedown	Online services are protected against lawsuits related to third-party content if they follow the notice-and-takedown procedure	Incentivizes online services to takedown content, even if it is permitted, to avoid liability	Higher content moderation costs raise the barrier to entry for new online services	Victims of illegal activity online could report it and have it removed	Victims of harmful activity online could report it and have it removed
Exempt State Criminal Law	Online services are protected against civil but not criminal lawsuits	State laws could incentivize online services to censor some types of speech	Higher legal costs raise the barrier to entry for new online services	Online services could face criminal liability for content or conduct that breaks state laws	Does not affect harmful, legal activity
Expand Federal Criminal Law	Online services and users are still protected against lawsuits related to third-party content	Online services can still determine what content is permitted without risk of frivolous lawsuits	Organizations can still build services and business models based on lawful user-generated content	Online services could face criminal liability for content or conduct that breaks new federal laws (e.g., soliciting revenge porn)	Does not target harmful, but legal, activity

Proposal	Impact on Nuisance Lawsuits	Impact on Protected Speech	Impact on Innovation	Impact on Illegal Activity	Impact on Harmful, but Legal, Activity
Expand Federal Civil Enforcement	Online services and users are protected from most lawsuits related to third-party content, but not from civil enforcement action brought by the federal government	Online services can still determine what content is permitted as long as it does not violate federal criminal law	Organizations can still build services and business models based on lawful user-generated content	The federal government can bring civil enforcement actions against online services for knowingly failing to remove and report illegal third-party content	Does not target harmful, but legal, activity
Eliminate the "Or Otherwise Objectionable" Clause	Establishes a stricter set of requirements for online services to avoid lawsuits related to removing third-party content	Online services would likely remove less speech	Organizations have less freedom to develop content moderation practices that work best for their communities	Online services still are not subject to state criminal law and have no civil liability for illegal activity of their users	Online services could face liability for removing harmful, but legal, speech and would likely remove less
Establish "Good Faith" Requirement	Online services cannot dismiss cases against them if plaintiffs claim they did not act in good faith or take reasonable steps to address unlawful uses of their services	May incentivize online services to censor controversial speech	Higher legal costs raise the barrier to entry for new online services	If plaintiffs prove an online service did not act in good faith, the service is liable for illegal activity	If plaintiffs prove an online service did not act in good faith, the service is liable for harmful activity
ITIF Proposal	Online services are protected against financial liability for third-party content if they implement standard industry measures	Online services can determine what content is permitted without significant risk from frivolous lawsuits	Different types of online services can develop their own standard industry measures to address unique concerns	Bad actors (i.e. online services not acting in good faith) will face liability and be subject to injunctive relief	Selective expansion of federal law will make certain harmful activities illegal (e.g. revenge porn)

RECOMMENDATIONS

Any reform to Section 230 should preserve the fundamental principle that liability for content should reside with the content creator. In addition, it is important that any reforms preserve online innovation, encourage content moderation, avoid targeting lawful speech, and maintain a consistent national standard for online intermediary liability.[53]

To accomplish this, updates to Section 230 should focus on ensuring online platforms are held responsible for their own conduct to minimize harms from illegal activity on their platforms. To that end, there are three steps Congress can take.

1. Create a Good Faith Requirement for Section 230(c)(1)

Congress should add a good faith provision to Section 230(c)(1). For example, Congress could amend the text to say (new text in brackets): "No provider or user of an interactive computer service [acting in good faith] shall be treated as the publisher or speaker of any information provided by another information content provider." This should be a narrow amendment.

The purpose of adding a good faith provision would be to minimize the risk that bad actors benefit from Section 230 protections. The wording is open-ended by design to give courts sufficient flexibility to limit the scope of Section 230 when it would advance unlawful activity. For example, an online service that hosts some illegal third-party content could, and should, be treated differently than one that to a reasonable person appears designed expressly for that purpose. In addition, this narrowing of Section 230 liability protection could help ensure online services are held responsible for their own conduct, while still protecting them from liability to their users. It also makes them more accountable for their own commitments. For example, a court may find that an online service that deliberately fails to enforce its terms of service prohibiting unlawful content, or selectively enforces it, is not acting in good faith.

2. Establish a Voluntary Safe Harbor Provision for Adherence to Standard Industry Measures

The biggest problem with adding a good faith provision is it would make it more difficult for defendants to get courts to dismiss nuisance lawsuits. Instead of merely demonstrating that they have liability immunity because of Section 230, they would also have to meet the higher burden of demonstrating that they have been acting in good faith, making it more expensive to defend themselves against lawsuits and increasing the risk that organizations will limit third-party content to avoid liability.

To address this concern, Congress should also establish an optional safe harbor provision online services could comply with to limit their financial liability. Importantly, this safe harbor provision should be entirely voluntary, not include an "actual knowledge" standard or an explicit takedown requirement, and avoid imposing a general monitoring obligation. Including an actual knowledge standard, takedown requirements, or a general monitoring obligation as a condition of the safe harbor would likely motivate online services to be unnecessarily overbroad in removing lawful content.

As a voluntary provision, all providers and users would still benefit from the general liability shield offered by Section 230; however, those at particular risk of nuisance lawsuits, including both start-ups and large platforms, could take additional steps to minimize their financial exposure.

Instead, the optional safe harbor provision should apply to online services that adhere to "standard industry measures" to prevent illegal activity on its services. Similar to the "standard technical measures" outlined in the DMCA, these standard industry measures should be developed pursuant to a broad consensus of service providers in an open, fair, voluntary, and multi-stakeholder process; available to any provider on reasonable and non-discriminatory terms, and not impose substantial costs on service providers or substantial burdens on their systems or networks. Different standard industry measures could be developed for different types of online providers, as long as they meet these basic requirements. For example, social networks, online retailers, and cloud hosting providers may have different risks and countermeasures for their respective online services.

The Department of Commerce would certify that the standard industry measures were developed according to an acceptable multi-stakeholder process—such as inclusion of a sufficient number of industry, civil society, and government stakeholders—but would not have the authority to directly approve or deny the specific conditions included as part of the standard industry measures. This division of responsibility would ensure that no future administration could force certain companies to adopt specific technical measures, such as a ban on end-to-end encryption, in order to receive liability protection for third-party content. Online service providers that want to avail themselves of the safe harbor would then be responsible for providing to the Department of Commerce a third-party audit confirming their adherence to an approved set of standard industry measures.

The goal of the safe harbor would be to provide sufficient flexibility for different types of online services to develop best practices to address the potential vulnerabilities users may exploit in their services to conduct illegal or harmful activity. However, the provision is intentionally optional so online services that have a low-risk exposure—such as not having significant third-party content—or their own effective content moderation practices would not have to adopt these measures if they minimized their liability exposure more efficiently through other means. Similarly, this would avoid imposing a significant regulatory cost on start-ups that may choose to forgo adopting these measures until they have established a viable online service.

Finally, by only limiting financial liability, this would still leave the door open for injunctive relief against an online provider. This would ensure that if courts found that online providers were not acting in good faith, they could still require these providers to take down specific third-party content, thereby ensuring that the safe harbor would not prevent courts from stopping harmful activity.

3. Selectively Expand Federal Criminal Law

Perhaps one of the biggest problems with Section 230 is that if something is not illegal at the federal level, there are few remedies available to victims to punish sites that encourage that behavior from users. The clearest example of this is the distribution of sexually explicit images without the subject's consent, or revenge porn, which is illegal in most states, yet is not illegal at the federal level.[54] In the absence of a criminal law for revenge porn, victims have little to no recourse against sites that may encourage other users to post this material. (Those who have been prosecuted essentially for running revenge porn websites have been convicted on other charges, such as identity theft and extortion.)[55]

In these cases, the solution should not be to pare back Section 230 protections or allow individual states to set policy for the entire country, but rather to act expeditiously to pass federal criminal law reforms to address emerging problems, such as revenge porn. Expanding federal criminal law would ensure online services can be held liable for aiding and abetting those engaging in this type of nefarious conduct.

Taken together, these three measures—creating a good faith requirement, establishing an optional safe harbor, and expanding federal criminal law—would reform online intermediary liability to reduce illegal activity, as well as harmful, but legal, activity, while protecting speech and innovation online, and not driving up costs for online services from nuisance lawsuits. It is important to note, however, that these proposals, particularly the establishment of a good faith requirement or a safe harbor provision are both problematic on their own: a good faith requirement would make it harder to dismiss nuisance lawsuits, while a safe harbor would raise regulatory costs and give regulators too much control over speech on platforms. However, if pursued jointly as part of a Section 230 reform, they would address the weaknesses of implementing either proposal independently by limiting nuisance lawsuits, encouraging industry best practices, and holding bad actors responsible.

CONCLUSION

The Internet has changed since Section 230's passage over two decades ago, and it makes sense to revisit and update the law in order to promote greater accountability. However, many of Section 230's foundational principles remain the same. Strong intermediary liability protection is still necessary to promote continued innovation and growth, protect users' freedom of expression, preserve competition and the free market online, and incentivize the moderation of harmful content.

Congress faces a wide spectrum of options for how it could change the law for online intermediary liability. Any changes to Section 230 should focus on reducing harmful and illegal activity without impeding any of these goals. However, many proposed reforms do not meet the standard of preserving innovation, free speech, competition, and good faith content moderation. A balanced, multi-pronged solution consisting of a good faith requirement, an optional safe harbor, and an expansion of federal criminal law would increase accountability and prevent bad actors from taking advantage of Section 230's liability shield, while protecting the many legitimate online services millions of Americans use for communication, education, political discourse, entertainment, and commerce on a daily basis.

Strong intermediary liability protection is still necessary to promote continued innovation and growth, protect users' freedom of expression, preserve competition and the free market online, and incentivize the moderation of harmful content.

Section 230 is one of the foundational laws of the Internet and updating it without undermining its benefits for online services and their users is a challenging but crucial task. Congress should move cautiously, yet purposefully, forward in an effort to update this important law to ensure companies take responsibility for harmful content and conduct while maintaining Section 230's protections for free speech and innovation.

While this report proposes a balanced reform to Section 230 that would address many of the concerns surrounding the United States' current approach to online intermediary liability, the debate surrounding Section 230 has also brought to the surface concerns surrounding online political speech. Or more accurately, the debate around political speech has led many to propose reforming Section 230, either out of a belief that changes could force platforms to moderate political speech differently or that the threat of Section reforms could spur them to revise their content moderation policies on political speech on their own. But as noted, many policymakers on the right believe large social media platforms remove too much content, especially conservative speech, while those on the left argue that these platforms do not remove enough, especially hate speech and misinformation. There is virtually no way that a change to Section 230 can address the concerns of both sides.

Resolving the debate over online political speech is an important issue, but one that should be addressed outside of the debate over Section 230. ITIF will address these issues in a separate, forthcoming report on online political speech.

About the Authors

Ashley Johnson (@ashleyjnsn) is a policy analyst at ITIF. She researches and writes about Internet policy issues such as privacy, security, and platform regulation. She was previously at Software.org: the BSA Foundation and holds a master's degree in security policy from The George Washington University and a bachelor's degree in sociology from Brigham Young University.

Daniel Castro (@CastroTech) is vice president at ITIF and director of its Center for Data Innovation. He writes and speaks on a variety of issues related to information technology and Internet policy, including privacy, security, intellectual property, Internet governance, e-government, and accessibility for people with disabilities.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent, nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized by its peers in the think tank community as the global center of excellence for science and technology policy, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

For more information, visit us at www.itif.org.

ENDNOTES

1. Robert D. Atkinson et al., "A Policymaker's Guide to the 'Techlash'—What It Is and Why It's a Threat to Growth and Progress" (ITIF, October 2019), https://itif.org/sites/default/files/2019-policymakers-guide-techlash.pdf.
2. Sarah Jeong, "A New Bill to Fight Sex Trafficking Would Destroy a Core Pillar of Internet Freedom," *The Verge*, August 1, 2017, https://www.theverge.com/2017/8/1/16072680/cda-230-stop-enabling-sex-traffickers-act-liability-shield-senate-backpage; "Section 230 of the Communications Decency Act," Electronic Frontier Foundation, accessed February 7, 2020, https://www.eff.org/issues/cda230; Matt Laslo, "The Fight Over Section 230—and the Internet as We Know It," *Wired*, August 13, 2019, https://www.wired.com/story/fight-over-section-230-internet-as-we-know-it/.
3. Elliot Harmon, "Changing Section 230 Would Strengthen the Biggest Tech Companies," *The New York Times*, October 16, 2019, https://www.nytimes.com/2019/10/16/opinion/section-230-freedom-speech.html.
4. Jack M. Balkin, "Free Speech and Hostile Environments," *Yale Law School Faculty Scholarship Series* 253 (1999): 2, https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1252&context=fss_papers.
5. "H.R.8896 - AOC Act," Congress.gov, accessed January 12, 2021, https://www.congress.gov/bill/116th-congress/house-bill/8896/.
6. Danielle Citron, "Tech Companies Get a Free Pass on Moderating Content," *Slate*, October 16, 2019, https://slate.com/technology/2019/10/section-230-cda-moderation-update.html.
7. "Section 230 Workshop – Nurturing Innovation or Fostering Unaccountability?", YouTube video, 2:31:50, posted by the U.S. Department of Justice, February 19, 2020, https://www.justice.gov/opa/video/section-230-workshop-nurturing-innovation-or-fostering-unaccountability.
8. Matthew Ingram, "The myth of social media anti-conservative bias refuses to die," *Columbia Journalism Review*, August 8, 2019, https://www.cjr.org/the_media_today/platform-bias.php.
9. Anshu Siripurapu, "Trump and Section 230: What to Know," *Council on Foreign Relations*, December 2, 2020, https://www.cfr.org/in-brief/trump-and-section-230-what-know.
10. Ibid., 2:17:20.
11. Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991); Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 24, 1995).
12. Atkinson et al., "A Policymaker's Guide."
13. 47 U.S.C. § 230(c)(1) (1996).
14. Donald Trump, "Executive Order on Preventing Online Censorship," *The White House*, May 28, 2020, whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/.
15. Sacha Baron Cohen, "The 'Silicon Six' Spread Propaganda. It's Time to Regulate Social Media Sites," *The Washington Post*, November 25, 2019, https://www.washingtonpost.com/outlook/2019/11/25/silicon-six-spread-propaganda-its-time-regulate-social-media-sites/.
16. "Defeating Disinformation Series: Social Media Regulation Around the World," YouTube video, 45:30, posted by the Woodrow Wilson International Center for Scholars, February 5, 2020, https://www.wilsoncenter.org/event/defeating-disinformation-series-social-media-regulation-around-world.
17. "Section 230 Workshop," YouTube video, 3:43:20.

18. Aja Romano, "A New Law Intended to Curb Sex Trafficking Threatens the Future of the Internet as We Know It," Vox, July 2, 2018, https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom.
19. 47 U.S.C. § 230(e) (1996).
20. "Warner, Hirono, Klobuchar Announce the SAFE TECH Act to Reform Section 230," Office of Senator Mark R. Warner, February 5, 2021, https://www.warner.senate.gov/public/index.cfm/2021/2/warner-hirono-klobuchar-announce-the-safe-tech-act-to-reform-section-230.
21. Romano, "A New Law."
22. 17 U.S.C. § 512(g)(2)(C) (1998).
23. "S.4066 - PACT Act," Congress.gov, accessed January 25, 2021, https://www.congress.gov/bill/116th-congress/senate-bill/4066.
24. Jennifer M. Urban, "Notice and Takedown in Everyday Practice" (Berkeley Law, April 2017), 13, https://www.law.berkeley.edu/wp-content/uploads/2017/02/2017-04-21_Takedown_BLCT-Platform-Conference_for-group-deck2.pdf.
25. Bruce Boyden, "The Failure of the DMCA Notice and Takedown System: A Twentieth Century Solution to a Twenty-First Century Problem" (GMU Center for the Protection of Intellectual Property, December 2013), 1, https://sls.gmu.edu/cpip/wp-content/uploads/sites/31/2013/08/Bruce-Boyden-The-Failure-of-the-DMCA-Notice-and-Takedown-System1.pdf.
26. Mark Warner, "Potential Policy Proposals for Regulation of Social Media and Technology Firms," https://www.warner.senate.gov/public/_cache/files/d/3/d32c2f17-cc76-4e11-8aa9-897eb3c90d16/65A7C5D983F899DAAE5AA21F57BAD944.social-media-regulation-proposals.pdf.
27. Mike Masnik, "Beto O'Rourke Joins The Silly Parade Of Confused Politicians Looking To Destroy Section 230," *Techdirt*, August 19, 2019, https://www.techdirt.com/articles/20190816/17304742801/beto-orourke-joins-silly-parade-confused-politicians-looking-to-destroy-section-230.shtml.
28. John Villasenor, "Why creating an internet 'fairness doctrine' would backfire," *Brookings*, June 24, 2020, https://www.brookings.edu/blog/techtank/2020/06/24/why-creating-an-internet-fairness-doctrine-would-backfire/.
29. "S.4066 - PACT Act," Congress.gov.
30. "H.R.492 - Biased Algorithm Deterrence Act of 2019," Congress.gov, accessed January 12, 2020, https://www.congress.gov/bill/116th-congress/house-bill/492.
31. "H.R.8515 - Don't Push My Buttons Act," Congress.gov, accessed January 12, 2020, https://www.congress.gov/bill/116th-congress/house-bill/8515.
32. "H.R.8922 - Break Up Big Tech Act of 2020," Congress.gov, accessed 12, 2020, https://www.congress.gov/bill/116th-congress/house-bill/8922.
33. "S.3398 - EARN IT Act of 2020," Congress.gov, accessed June 4, 2020, https://www.congress.gov/bill/116th-congress/senate-bill/3398.
34. Ashley Johnson, "A Backdoor Attempt to Require Backdoors to Encryption," *Morning Consult*, March 11, 2020, https://morningconsult.com/opinions/a-backdoor-attempt-to-require-backdoors-to-encryption/.
35. 47 U.S.C. § 230(e) (1996).
36. "Section 230 Workshop," YouTube video, 2:39:05.
37. 47 U.S.C. § 230(e)(1) (1996).
38. "State AGs Support Amendment to Communications Decency Act," National Association of Attorneys General, May 23, 2019, https://www.naag.org/policy-letter/state-ags-support-amendment-to-communications-decency-act/.

39. "46 States + DC + One Territory Now Have Revenge Porn Laws," Cyber Civil Rights Initiative, accessed February 26, 2020, https://www.cybercivilrights.org/revenge-porn-laws/.

40. 18 U.S.C. § 1028, as amended by Pub. L. 105-318, 112 Stat. 3007 (Oct. 30, 1998).

"Citizen's Guide to U.S. Federal Law on Child Pornography," Department of Justice, May 28, 2020, https://www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography.

18 U.S.C. § 1030, as amended by Pub. L. 99-474, 100 Stat. 1213 (Oct. 16, 1986).

18 U.S.C. § 2422.

18 U.S.C. § 2425.

41. Aja Romano, "A New Law Intended to Curb Sex Trafficking Threatens the Future of the Internet as We Know It," Vox, July 2, 2018, https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom.

42. "Department of Justice's Review of Section 230 of the Communications Decency Act of 1996," Department of Justice, accessed January 13, 2021, https://www.justice.gov/ag/department-justice-s-review-section-230-communications-decency-act-1996.

43. "Department of Justice's Review of Section 230 of the Communications Decency Act: Section by Section," Department of Justice, accessed January 13, 2021, https://www.justice.gov/file/1319326/download.

44. 47 U.S.C. § 230(c)(2) (1996).

45. "H.R.4207 - Stop the Censorship Act," Congress.gov, accessed January 12, 2021, https://www.congress.gov/bill/116th-congress/house-bill/4027/.

46. "S.4534 - Online Freedom and Viewpoint Diversity Act," Congress.gov, accessed January 13, 2021, https://www.congress.gov/bill/116th-congress/senate-bill/4534/text.
"S.4632 - Online Content Policy Modernization Act," Congress.gov, accessed January 13, 2021, https://www.congress.gov/bill/116th-congress/senate-bill/4632.

47. Sabrina Hersi Issa, "Trump's Twitter ban renews calls for tech law changes by many who don't get tech or the law," *NBC News*, January 11, 2021, https://www.nbcnews.com/think/opinion/trump-s-twitter-ban-renews-calls-tech-law-changes-many-ncna1253627.

48. Ashley Johnson, "New Attempts to Amend Section 230 Would Impede Content Moderation When It Is Needed Most" (ITIF September 24, 2020), https://itif.org/publications/2020/09/24/new-attempts-amend-section-230-would-impede-content-moderation-when-it.

49. 47 U.S.C. § 230(c)(2) (1996).

50. E-Ventures Worldwide v. Google, No. 2:14-cv-646-FtM-29CM, 2016 U.S. Dist. LEXIS 62855 (M.D. Fla. May 12, 2016).

51. Danielle Keats Citron, Benjamin Wittes, "The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity," *Fordham Law Review* 86, no. 2 (2017), https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5435&context=flr.

52. "S.3983 - Limiting Section 230 Immunity to Good Samaritans Act," Congress.gov, accessed January 12, 2021, https://www.congress.gov/bill/116th-congress/senate-bill/3983.

53. "Liability for User-Generated Content Online: Principles for Lawmakers," July 11, 2019, https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2992&context=historical.

54. Daniel Castro and Alan McQuinn, "Why and How Congress Should Outlaw Revenge Porn" (ITIF, July 2015), http://www2.itif.org/2015-congress-outlaw-revenge-porn.pdf.

55. Associated Press in San Diego, "Revenge porn website operator jailed," *The Guardian*, April 4, 2015, https://www.theguardian.com/us-news/2015/apr/04/revenge-porn-website-operator-jailed.