The Heritage Foundation

ISSUE BRIEF

No. 6020 | OCTOBER 27, 2020

CENTER FOR TECHNOLOGY POLICY

Section 230—Mend It, Don't End It

Klon Kitchen

KEY TAKEAWAYS

Congress should refine Section 230 of the Communications Decency Act to ensure that markets and civil discourse remain free and fair.

Google, Facebook, Twitter, and other tech firms have squandered the public trust with inconsistent and often political moderation and censorship of user content.

Section 230 must be carefully refined to better fit the statute's original intent and to restrain potential abuses of its protections.

"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

These words in Section 230 of the Communications Decency Act (CDA) are at the heart of an increasingly important public debate about technology, economics, and society. They have been called "the 26 words that created the Internet"[1] and an "outlandish power over speech without accountability."[2] There is a large policy gap between these two views, and policymakers on both sides of the aisle are offering proposals to change this law that could fundamentally reshape the American technology industry.

Some believe that large tech companies are not keeping their part of the deal that critics say undergirds Section 230. These companies, it is argued, are politically biased and are exercising

editorial judgments on which content they will, and will not, allow on their platforms, and that these judgments violate the law's precondition of platform neutrality.

Others, however, say that this precondition of neutrality never existed and that removing these liability protections will effectively kill the American technology industry that is the beating heart of the U.S. economy.

Still others believe these large Internet companies—especially those that host social media platforms—are sources of social degradation and those who hold this view are happy to threaten Section 230's protections as a way of coercing these companies into more acceptable behavior.

All of these perspectives are enabled by vagaries surrounding the text of the law, the intent behind it, and the relative values and risks posed by large Internet platforms.

What Americans Need to Know About Section 230

The liability protections at issue are in Section 230 of the CDA, which is itself part of the Telecommunications Act of 1996. The intent of Section 230 was made clear by its authors, then-Representatives Christopher Cox (R–CA) and Ron Wyden (D–OR), who said they wanted "to encourage telecommunications and information service providers to deploy new technologies and policies" for filtering or blocking offensive materials online.[3] This proposal was in direct response to the court case *Stratton Oakmont, Inc. v. Prodigy Services Co.*[4]

Prodigy was an online bulletin board in the early days of the Internet that used software to filter profanity from its pages. A Prodigy user posted derogatory comments about the investment firm Stratton Oakmont (the investment firm made famous by the 2013 movie *The Wolf of Wall Street*). Stratton Oakmont successfully sued Prodigy for defamation for $200 million, with the court ruling that Prodigy's efforts to remove obscene content made it a publisher, and therefore responsible for *not* removing defamatory information about the investment firm.

Prodigy lost the case not because it removed material, but because it had—from the court's perspective—done so incompletely. Representatives Cox and Wyden were concerned that this precedent would disincentivize online service providers from removing offensive content, and also put the brakes on Internet innovation by subjecting companies to endless lawsuits over user-generated content. Cox and Wyden drafted Section 230 and incorporated it as an amendment to the CDA.

Section 230(c) reads as follows:

> **(c) Protection for "Good Samaritan" blocking and screening of offensive material**
>
> **(1) Treatment of publisher or speaker**
>
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
>
> **(2) Civil liability**
>
> No provider or user of an interactive computer service shall be held liable on account of—
>
> **(A)** any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> **(B)** any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

Section 230(c)(2)(a) is the main immunity clause and a focus of the current debate, specifically what is meant by "good faith" and "otherwise objectionable." In law, *good faith* is an abstract and general term used to describe "sincere belief of motive without malice or the desire to defraud others."[5] The phrase "otherwise objectionable" is clearly a continuation of the preceding list containing "obscene," "lewd," "lascivious," "filthy," "excessively violent," and "harassing." Typically, "otherwise objectional" would be interpreted using the legal canon of construction *ejusdem generis* ("of the same kind"), meaning that content that a reasonable person would find offensive that is of the same kind as those described in the preceding list.

To put it simply, the main immunity clause intends to protect Internet companies from liability for removing material that a reasonable person would find objectionable, so long as it is done in a manner not intended to harm or to defraud others. Subsequent courts, however, have extended these protections well beyond their intended boundaries.

While the Supreme Court has declined to engage the meaning of Section 230, state and lower courts have consistently ruled that it offers a very broad liability shield. Often citing Section 230's "findings" and "policy" sections, which call for a "vibrant and competitive free market" and "myriad avenues for intellectual activity,"[6] these courts have built a strong First Amendment standard for interpreting the protections afforded to any company's online presence.

Section 230 does *not* shield companies from federal laws against crimes such as trafficking in child pornography, drug trafficking, or terrorism; however, the courts' broad interpretation has allowed websites, such as Backpage.com, to avoid liability for hosting "80 percent of the online advertising for illegal commercial sex in the United States."[7] Other examples, as catalogued by Danielle Citron and Benjamin Wittes,[8] include the following:

- A "revenge porn" website devoted to posting nude images without consent;[9]
- A gossip site collecting and disseminating "dirt" on private individuals;[10]
- A message board knowingly facilitating illegal activity and refusing to collect information on that illegal activity;[11]
- A website hosting sex-trade advertisements whose design and technical setup specifically prevented the detection of sex-trafficking;[12] and
- A "hook-up" site that ignored more than 50 reports that one of its subscribers was impersonating another individual and falsely suggesting that individual's interest in rough sex as part of a "rape fantasy," resulting in hundreds of strangers confronting that person for sex at work and home.[13]

Regarding the other liability provision in Section 230(c)(2)(b), Congress is clearly encouraging the removal of objectionable materials by encouraging the sharing of "technical means to restrict access to material described" in Section 230(c)(2)(a).

Section 230 is clearly intended to incentivize Internet companies and websites to proactively remove objectionable content by providing them with a liability shield from continuous and presumably frivolous lawsuits from aggrieved users. The statute's vague language and subsequently broad

judicial interpretations have, however, led to a situation where some Internet companies are overly insulated from accountability and are reasonably suspected of not meeting Section 230's good faith standard.

This is why it is time to refine Section 230.

Why Section 230 Should Be Refined—Now

Section 230's original intent of incentivizing and protecting the removal of obscene materials online continues to be good policy and a noble objective—thus, the statute should be maintained. But, the evolution of the Internet, and growing concerns about political bias online, require that the statute be clarified and refined. Specific proposed changes are provided in "Policy Recommendations" below; first, it is helpful to briefly explain why these changes are necessary now.

First, the Internet is more central to American life than could have been envisioned when the CDA was passed, and the law should reflect this reality. In 1996, approximately 0.9 percent of the global population (36 million people) was on the Internet. Today, 62 percent of mankind (4.8 billion people) is online.[14] In 1996, Americans with an Internet connection spent an average of 30 minutes online per month. Today, it is about 27 hours per month.[15] Today, more than 34 percent of Americans prefer to get their news online, with nearly twice as many getting their news from social media than from newspapers.[16] These and other Internet trends demonstrate that the World Wide Web is no longer simply a collection of online chats or bulletin boards. It is, instead, a growing public square where Americans' economic, social, and political lives are expressed, debated, and shaped.

Second, there is growing concern that Internet companies—particularly social media companies—are abusing their influence and Section 230 to skew public debate and to marginalize political speech with which they do not agree. Polling demonstrates this is a bipartisan concern.[17]

For example, three-quarters of U.S. adults believe that social media companies "intentionally censor political viewpoints that they find objectionable,"[18] and 72 percent say that social media companies "have too much power and influence in politics today."[19] And, while 80 percent of Republicans have little or no confidence "in social media companies to determine which posts on their platforms should be labeled as inaccurate or misleading," 52 percent of Democrats have this view.[20]

The reasons for this widescale mistrust are myriad and it is impossible to adjudicate all of the claims of online bias and mistreatment. Following are but three examples that illustrate why these companies are hemorrhaging trust:

1. In September, a series of pro-conservative political advertisements were labeled as "missing context" and prevented from running as paid advertisements on Facebook.[21] The fact-checker, PolitiFact, justified the label by saying the claims in the advertisement could not be assessed because "we can't predict the future." While not ruling the advertisement as "false," the context label achieved the same outcome: The advertisements were stopped. This gaming of the fact-checking system is now common among left-leaning "fact-checkers."

2. In May, Twitter added a "Get the Facts" label to a tweet by President Donald Trump[22] concerning mail-in ballots and election fraud—the first time the social media company had ever added such a label to a tweet by an elected official. The company justified the decision by asserting that the President's post was misleading; however, the issue of mail-in ballots and election integrity is legitimately debated, and Twitter's actions undoubtedly suggest otherwise. Furthermore, similar labels have not been added to outrageous liberal claims. For example, Senator Elizabeth Warren (D–MA) recently tweeted that "Racism isn't a bug of Donald Trump's administration—it's a feature. Racism is built into his platform."[23]

3. Last year, an internal e-mail from a Google employee referred to conservative commentator Ben Shapiro and others as "Nazis," saying, "I don't think correctly identifying far-right content is beyond our capabilities." The e-mail appears to have been a part of discussions within the company's "transparency and ethics" group.[24]

Since conservatives are largely thriving online, some may not find the examples above compelling; but, it should be sufficient to simply recognize these companies' failure to secure public confidence or to conduct themselves in a coherent fashion that would entitle them to the benefit of the doubt. Moreover, by editing or adding labels to content posted by others, these companies are blurring the lines in unacceptable ways between being a mere conduit of content and being a "publisher or speaker" of the revised content.

Some will rightly argue that these are private companies that have no obligation to be "fair" or to provide their services in any other manner than in the one of their choosing. This, of course, is true. But, in the context of Section 230, it is important to remember that liability protection is a benefit, and the lack of this protection is not a penalty. This benefit is only given to

online sources; real-world newspapers, bulletin boards, and other similar sources enjoy no such protections. For now, bestowing such a benefit makes sense; however, as one observer has said, "Section 230 immunity is a legal privilege to be earned by compliance with the attendant conditions. If an entity fails to comply, that just means it does not get the privilege; it does not mean the entity is being denied a right or being punished."[25]

It is high time that the scope and conditions of Section 230 are clarified.

A Word of Warning

While this *Issue Brief* joins others in calling for changes to Section 230, it does not align with all requested changes or all justifications offered for these changes. Some claim that social media companies should be regulated as "public utilities." Others argue that federal antitrust actions should be taken against them. The first assertion is difficult to justify under the normal meaning of "public utility" because these companies do not have a government-imposed monopoly, and all of these businesses have multiple competitors in their respective markets. The second assertion is a separate issue altogether. Both arguments are often offered from a position of political grievance rather than strict policy analysis. While it is easy to empathize with such frustrations, this is an unwise approach to engaging an industry that constitutes nearly 7 percent of U.S. gross domestic product[26] and nearly 40 percent of the S&P 500.[27]

Even more fundamentally, conservatives should be especially mindful of potential unintended consequences of overly aggressive or ill-considered changes. Some social media companies could choose not to moderate any content on their platforms out of fear that, like Prodigy, they would be held liable for content they did not remove. In a world where every minute of every day Facebook users upload 147,000 photos, Twitter gains 319 new users, Instagram users post 347,222 stories, and YouTube creators upload 500 hours of video,[28] the fear of missing something is a reasonable concern. This "no moderation" standard could significantly increase the presence of pornography and other objectionable content on these platforms—the exact opposite of Section 230's intent.

On the other side of the spectrum, online communities could respond to increased liability by ratcheting up their content moderation, adopting a "no mercy" standard that, if past is prologue, could disproportionately impact conservative speech online. How likely is it, for example, that people will sue Facebook because a pro-life advertisement made them feel "unsafe"?

If handled carefully, Section 230 need not illicit these extreme responses; but, it is important that all parties undertake this reform with eyes wide open.

Policy Recommendations

Congress should update Section 230 of the CDA with the following proposed changes:

- **Define "good faith" more clearly.** The Department of Justice's proposed definition of "good faith," found in the "Ramseyer Draft Legislative Reforms to Section 230 of the Communications Decency Act,"[29] is a helpful example of such an explanation:

  > Good Faith:
  >
  > To restrict access to or availability of specific material "in good faith," an interactive computer service provider must–
  >
  > (A) Have publicly available terms of service or use that state plainly and without particularity the criteria the service provider employs in its content-moderation practices;
  >
  > (B) Restrict access to or availability of material consistent with those terms of service or use and with any official representation or disclosures regarding the service provider's content-moderation practices;
  >
  > (C) Not restrict access to or availability of material on deceptive or pretextual grounds, or apply its terms of service or use to restrict access to or availability of material that is similarly situated to material that the provider intentionally declines to restrict; and
  >
  > (D) Supply the provider of the material with timely notice describing with particularity the provider's reasonable factual basis for the restriction of access and a meaningful opportunity to respond, unless a law enforcement agency has asked that such notice not be made, or a provider reasonably believes that the material relates to terrorism or other criminal activity, or that such notice would risk imminent harm to others.

- **Strike "otherwise objectionable" from Section 230(c)(2)(a).** As discussed, this vague language is the source of overly broad interpretations of the liability shield. While companies should certainly have the freedom to allow or to remove whatever content they choose, narrowing the applicability of Section 230 and its protections is prudent. To

preserve some flexibility, however, the sentence could also be changed to read as follows (changes are italicized).

> Any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user *has an objectively reasonable belief is* obscene, lewd, lascivious, filthy, excessively violent, or harassing, whether or not such material is constitutionally protected.

- **Clarify the line between acceptable editing and becoming a publisher who no longer enjoys Section 230 protections.** A number of common practices—such as labeling, delisting, and context commentaries—are not technically understood as content editing; however, they have clear effects on how content is accessed, understood, and shared. The updated Section 230 should address this issue and draw a clearer line on these practices and on what does, and does not, violate the editorial preconditions of Section 230 protections.

- **Clarify "no effect" on anti-terrorism, child sex abuse, and cyber-stalking laws.** Under "Effects on Other Laws," the explicit identification of anti-terrorism, child sex abuse, and cyber-stalking law carve-outs appropriately incentivizes the moderation of such content and removes ambiguities concerning an "interactive computer service's" responsibilities on these matters. See the "Ramseyer Draft Legislative Reforms" for proposed language.[30]

- **Create a "Bad Samaritan" carve-out.** Congress should adopt the Justice Department's proposed "Bad Samaritan" carve-out. This provision specifically removes liability protections from any interactive computer service that acts "purposefully with the conscious object to promote, solicit, or facilitate material or activity...that the service provider knew or had reason to believe would violate Federal criminal law."[31] Such a change moves Section 230s protections closer to its original intent.

- **Not make liability protections contingent on "exceptional access" or similar law enforcement cooperation.** A number of legislative proposals seek to make Section 230's liability protections contingent on an interactive computer service's cooperation with law enforcement—such as providing law enforcement with "exceptional access" to encrypted devices and data. To be clear, the case for special

access to encrypted materials can have noble objectives and intentions; but technology has changed to make such access detrimental to cybersecurity and data integrity, with no guarantee of success. Furthermore, there are robust mechanisms for handling law enforcement data requests and it is counterproductive to conflate these issues with Section 230's liability protections.

- **Enact a sunset provision for Section 230.** Section 230 should have a "sunset" provision requiring Congress to re-enact this law every seven years. Seven years provides sufficient stability to allow companies to plan and to operate accordingly, while the sunset prevents these companies from growing complacent with this privilege. The sunset also provides a built-in opportunity to ensure that Section 230 reflects the inevitable evolution of applicable technologies and services.

Conclusion

Refining Section 230 is the best way to fan the flames of economic freedom and creativity while protecting individual and corporate freedom of speech. It is also essential that the nation's technology laws recognize and account for the evolving challenges of a nearly ubiquitous Internet that bears little resemblance to the nascent World Wide Web of the mid-1990s. While the online world is not the totality of the public square, it is an ever-growing portion of that square, and good governance and human thriving require that this important statute be better suited for current times and needs.

Klon Kitchen is Director of the Center for Technology Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.

Endnotes

1. Jeffery Kosseff, *The Twenty-Six Words That Created the Internet* (Cornell, NY: Cornell University Press, 2019).
2. News release, "Senator Hawley Announces Bill Empowering Americans to Sue Big Tech Companies Acting in Bad Faith," Josh Hawley, U.S. Senator for Missouri, June 17, 2020, https://www.hawley.senate.gov/senator-hawley-announces-bill-empowering-americans-sue-big-tech-companies-acting-bad-faith (accessed October 23, 2020).
3. Senate Report No. 104-23.
4. No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).
5. TheFreeDictionary.com, "Legal Dictionary: Good Faith," https://legal-dictionary.thefreedictionary.com/good+faith (accessed October 21, 2020).
6. See, for example, *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1099 (9th Cir. 2009) (relying on §§ 230(a)(3) and 230(b)(2) to say that free speech values are the foundation of the immunity provisions).
7. Petition for Writ of Certiorari at 7, *Backpage*, 137 S. Ct. 622 (No. 16-276), 2016 WL 4610982.
8. This list is adapted from Danielle Citron and Benjamin Wittes, "The Internet Will Not Break: Denying Bad Samaritans §230 Immunity," *Fordham Law Review*, Vol. 86, No. 2, (2017).
9. Danielle Keats Citron, "Cyber Civil Rights," *Boston University Law Review*, Vol. 89, No. 61, https://www.bu.edu/law/journals-archive/bulr/volume89n1/documents/CITRON.pdf (accessed October 23, 2020).
10. *Jones v. Dirty World Entertainment Recordings LLC*, 755 F.3d 398, 402-03 (6th Cir. 2014).
11. Citron, "Cyber Civil Rights."
12. *Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 16 (1st Cir. 2016), *cert. denied*, 137 S. Ct. 622 (2017) (No. 16-267).
13. *Herrick v. Grinder*, No. 17-CV-932 (VEC), 2017 WL 744605, at *1 (S.D.N.Y. Feb. 24, 2017), and Andy Greenberg, "Spoofed Grinder Accounts Turned One Man's Life into a Living Hell," *Wired*, January 31, 2017, https://www.wired.com/2017/01/grinder-lawsuit-spoofed-accounts/#:~:text=Spoofed%20Grindr%20Accounts%20Turned%20One%20Man's%20Life%20Into%20a%20'Living%20Hell',-Grindr&text=That's%20when%20the%20man%20pulled,Herrick%20was%20unnerved (accessed October 23, 2020).
14. Internetworldstats.com, https://www.internetworldstats.com/emarketing.htm (accessed October 21, 2020).
15. Farhad Manjoo, "Jurassic Web: The Internet of 1996 Is Almost Unrecognizable Compared with What We Have Today," Slate.com, https://slate.com/technology/2009/02/the-unrecognizable-internet-of-1996.html (accessed October 21, 2020).
16. A. W. Geiger, "Key Findings About the Online News Landscape," Pew Research Center, September 11, 2019, https://www.pewresearch.org/fact-tank/2019/09/11/key-findings-about-the-online-news-landscape-in-america/ (accessed October 21, 2020).
17. Emily A. Vogels, Andrew Perrin, and Monica Anderson, "Most Americans Think Social Media Sites Censor Political Views," Pew Research Center, August 19, 2020, https://www.pewresearch.org/internet/2020/08/19/most-americans-think-social-media-sites-censor-political-viewpoints/ (accessed October 21, 2020).
18. Ibid., and Monica Anderson, "Most Americans Say Social Media Companies Have Too Much Power, Influence in Politics," Pew Research Center, July 22, 2020, https://www.pewresearch.org/fact-tank/2020/07/22/most-americans-say-social-media-companies-have-too-much-power-influence-in-politics/ (accessed October 21, 2020).
19. Anderson, "Most Americans Say Social Media Companies Have Too Much Power, Influence in Politics."
20. Vogels, Perrin, and Anderson, "Most Americans Think Social Media Sites Censor Political Views."
21. News release, "Heritage Experts: Facebook Is Allowing Political Partisans to Game 'Fact-Checking' Program," The Heritage Foundation, September 16, 2020, https://www.heritage.org/press/heritage-experts-facebook-allowing-political-partisans-game-fact-checking-program (accessed October 25, 2020).
22. Donald Trump (@RealDonaldTrump), "There is NO WAY (ZERO!) that Mail-In Ballots will be anything less than substantially fraudulent. Mail boxes will be robbed, ballots will be forged & even illegally printed out & fraudulently signed. The Governor of California is sending Ballots to millions of people, anyone....," Twitter, May 26, 2020, https://twitter.com/realDonaldTrump/status/1265255835124539392 (accessed October 27, 2020).
23. Elizabeth Warren (@ewarren), "Let's be clear: Racism isn't a bug of Donald Trump's administration—it's a feature. Racism is built into his platform. And we have the opportunity—the obligation—to vote it out." Twitter, October 22, 2020, https://twitter.com/ewarren/status/1319463898400030720 (accessed October 27, 2020).
24. James Rogers, "Ben Shapiro Slams Google Over Email Describing Him as a 'Nazi,'" FoxNews.com, June 26, 2019, https://www.foxnews.com/tech/ben-shapiro-slams-google-over-email-describing-him-as-a-nazi (accessed October 23, 2020).
25. Andrew McCarthy, "How to Put a Stop to Twitter's Game-Playing on Censorship," *National Review Online*, October 21, 2020, https://www.nationalreview.com/2020/10/washington-can-put-a-stop-to-twitters-game-playing-on-censorship/ (accessed October 21, 2020).

26. U.S. Bureau of Economic Analysis, "Measuring the Digital Economy: An Update Incorporating Data from the 2018 Comprehensive Update of the Industry Economic Accounts," April 2019, https://www.bea.gov/system/files/2019-04/digital-economy-report-update-april-2019_1.pdf (accessed October 21, 2020).
27. Amrith Ramkumar, "Tech's Influence Over Markets Eclipses Dot-Com Bubble Peak," *The Wall Street Journal*, October 16, 2020, https://www.wsj.com/articles/techs-influence-over-markets-eclipses-dot-com-bubble-peak-11602894413 (accessed October 21, 2020).
28. Domo.com, "Data Never Sleeps 8.0," https://www.domo.com/learn/data-never-sleeps-8 (accessed October 21, 2020).
29. U.S. Department of Justice, "Ramseyer Draft Legislative Reforms to Section 230 of the Communications Decency Act," September 23, 2020, https://www.justice.gov/file/1319331/download (accessed October 21, 2020).
30. Ibid.
31. Ibid.