SECTION 230 OF THE COMMUNICATIONS DECENCY ACT

POTENTIAL REFORMS AND IMPLICATIONS

BY SETH A. STERN

ALASHI / DIGITAL VISION VECTORS VIA GETTY IMAGES PLUS

Rare bipartisan consensus exists regarding the supposed need to repeal or reform § 230 of the Communications Decency Act, which largely immunizes social media outlets and other providers of "interactive computer services" from liability for third-party content.[1] It remains unclear what shape reforms might take, and when, but any significant change is likely to have implications not for the major social media outlets that have dominated headlines regarding § 230 reform, but for all internet users and providers. This article will discuss § 230's history, its current scope, common critiques of the immunity that it provides, and the reforms that have been proposed thus far.

Before § 230

In the early 1990s, courts grappled with the applicability of existing law to a new platform, the internet, where relatively small companies and even individuals hosted websites allowing real-time publication without the opportunity for editing. Some courts advocated caution to avoid impeding the development of new technologies, while others preferred not to disadvantage traditional media outlets, which are generally liable for content that they publish whether or not they authored it.

For example, one early case, *Cubby, Inc. v. CompuServe Inc.*, held that websites could be held liable for defamatory content posted by third parties if they "knew or had reason to know" of such content.[2] Another held that sites became vulnerable to liability if they held themselves out to the public as having the capability to monitor or remove unlawful content.[3] These and similar holdings meant that the best way for a provider to avoid liability was to bury its head in the sand and not make any effort to monitor or remove illegal content—let alone develop filtering technologies that, especially in their early stages, were sure to be flawed.

Enactment of § 230

In response to such cases, § 230 was enacted in 1996 "to promote the continued development of the Internet and other interactive computer services and other interactive media" and "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services."[4] Although Congress was particularly concerned with encouraging the development of technologies to prevent children from accessing inappropriate content,[5] § 230 is more commonly invoked as a defense against defamation and privacy claims.

Section 230 provides that "[n]o 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."[6] The immunity, however, is not absolute—a provider can lose its immunity if responsible, "in whole or in part, for the creation or development of [the] information" at issue.[7] This nuance has led to significant litigation to define the confines of § 230 immunity.

Cases Embracing—and Broadening—§ 230 Immunity

Courts quickly began to broaden the scope of § 230's immunity and renounce the pre–§ 230 case law discussed above.

The year after § 230's enactment, the U.S. Court of Appeals for the Fourth Circuit rejected the same argument that, for example, *Cubby* had endorsed and held that conditioning immunity on notice of unlawful content would undermine the goal of encouraging providers to self-regulate.[8] Similarly, the U.S. Court of Appeals for the Tenth Circuit held that emails demanding corrections did not cause the defendant to lose immunity as an information content provider.[9]

The only notable pushback came from the U.S. Court of Appeals for the Seventh Circuit, which suggested, in dicta, that to qualify for immunity, providers should be required to at least attempt to monitor and filter unlawful content.[10] That outlier view did not catch on at the time (although, as discussed later, it has been revived by recently proposed legislation).

Courts also limited the aforementioned exemption for providers responsible for the creation or development of the unlawful content. *Blumenthal v. Drudge*, for example, upheld immunity even though the provider paid a columnist accused of defamation for his content and advertised his columns as containing "gossip."[11] In *Donato v. Moldow*, the court upheld immunity even though the owner of the website in question commented on the third-party content, deleted some messages while allowing others, and selectively banned users.[12] Courts also rejected work-arounds to evade § 230, including attempts to treat online providers as places of public accommodation under Title II of the Civil Rights Act of 1964.[13]

More recently, courts have rejected arguments that social media sites lose immunity by applying algorithms that might promote, or lead users to access, unlawful content. *Force v. Facebook, Inc.*, for example, involved a claim that Facebook violated anti-terrorism laws by allowing alleged terrorist organizations to post content and then developing algorithms that would lead interested users to that content.[14] This kind of algorithmic sorting—and, relatedly, concerns about platforms' content neutrality—largely has driven recent calls for reform.

Cases Limiting § 230 Immunity

In addition to § 230's built-in exemptions, including for intellectual property violations and federal criminal law, some courts have chipped away at the scope of its immunity. Specifically, courts have held that providers may lose immunity when they prompt users for illegal content.

The U.S. Court of Appeals for the Ninth Circuit, in the 2008 case *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, held that the operator of the roommate-matching website www.roommates.com (Roommate) lost § 230 immunity because its user questionnaires required disclosure of the user's sex, sexual orientation, and familial status, as well as like disclosure of their preferred roommates, in violation of the Fair Housing Act (FHA).[15] Roommate was considered the information content provider

TIP: Attorneys should advise clients whose business models rely on a robust § 230 that the scope of immunity might become more limited going forward.

because it developed the questionnaire and, essentially, left users with no choice but to use its platform in an unlawful manner. Citing *Roommates.com*, the Tenth Circuit denied immunity against claims under the Federal Trade Commission (FTC) Act where a website was alleged to have paid researchers to acquire confidential telephone records for its directory because the site contributed materially to the alleged illegality.[16]

Subsequent cases limit the *Roommates.com* exception to situations where users *must* act unlawfully as opposed to merely being highly likely to do so. For example, another FHA case, *Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, upheld immunity because Craigslist merely allowed—rather than specifically prompted—discriminatory content.[17] Courts have also held sites like StubHub immune, even though it is hardly a secret that StubHub is used to scalp tickets, because StubHub leaves it up to the users to set their ticket prices.[18]

More recent cases have continued to chip away at § 230 immunity, albeit often in highly fact-specific contexts. The court in *Barnes v. Yahoo!, Inc.*, immunized Yahoo! for failing to remove private photographs and other materials posted by the plaintiff's ex-boyfriend but held that her promissory estoppel claims—arising from a Yahoo! executive's alleged promise to ensure that the content at issue was removed—were not subject to immunity because they did not treat Yahoo! as the publisher but rather sought to hold it to a verbal contract.[19]

In 2016, the Ninth Circuit held that § 230 did not bar a model's claim against an industry networking website that the site's operators, in violation of a California statute, failed to warn her that the website was used to identify targets for a rape scheme.[20] Last year, the Ninth Circuit held that the maker of Snapchat was not immune for claims that its "speed" filter—which allowed users to display the speed at which they were moving in real time—incentivized teens to drive recklessly, causing a tragic accident.[21]

These cases, although significant, do not address the concerns underlying current bipartisan calls for reform—i.e., concerns on the political right about Big Tech allowing political biases to censor conservatives and shape public discourse, and concerns on the left about algorithms that promote extremism and misinformation in order to increase clicks and drive profits.

Seth A. Stern *is an attorney with Funkhouser Vegosen Liebman & Dunn Ltd. in Chicago, focusing on commercial litigation and counseling for traditional media and social media issues. He is chair-elect of the TIPS Media, Privacy and Advertising Law Committee. He may be reached at sstern@fvldlaw.com.*

The § 230 Reform Movement

Although some older cases involved relatively large (for their time) defendants, like AOL or Yahoo!, many involved smaller chat rooms or bulletin boards that could not exist if required to monitor content for illegality in real time. The downside of immunity, in that context, was often limited to individuals being left without a viable remedy for defamatory content (which, in many cases, would have been seen by a fairly limited audience).

Public policy considerations have arguably changed given the rise of larger social media entities with the funds to be more proactive in policing third-party content and the development of technologies that would allow them to do so. Moreover, the growth of the internet means that concerns about individual reputational harm have given way to fears that social media can be used to spread mass disinformation and organize riots and coups. And social media outlets' editorial decisions have the potential to significantly affect public discourse and even swing election outcomes: the debate over Twitter's handling of Donald Trump's account is the most obvious example. Put simply, the stakes are much higher in 2022 than when § 230 was enacted over 25 years ago.

On the other hand, despite advances, no technology exists that can precisely target unlawful content in real time, and attempts to do so are likely to be both over- and underinclusive.

Despite the high stakes, both political parties, citing the aforementioned concerns about algorithmic sorting and content neutrality, generally favor § 230 reform. Some politicians have even called for § 230's repeal. During the last presidential election cycle, Trump, in his veto message to the House of Representatives for H.R. 6395 (the National Defense Authorization Act for Fiscal Year 2021), stated, "Section 230 facilitates the spread of foreign disinformation online, which is a serious threat to our national security and election integrity. It must be repealed."[22] Similarly, President Joe Biden stated, "It should be revoked because [Facebook] is not merely an internet company. . . . [It is] propagating falsehoods they know to be false."[23]

Despite such statements, most actual legislative proposals have been for targeted reforms—some more ambitious than others, but not outright repeals. Some examples include the following:

- On June 19, 2019, Senator Josh Hawley (R-MO) introduced the Ending Support for Internet Censorship Act (S. 1914), which would condition immunity for large tech companies on their acquiescence to an FTC audit to prove that their content-sorting algorithms and content-removal practices are politically neutral.[24]

- On January 22, 2021, Senator Joe Manchin (D-WV) introduced the See Something, Say Something Online

Act of 2021 (S. 27), aimed primarily at targeting online drug sales and other criminal activity.[25] It would require interactive computer services, in order to retain their immunity, to submit a suspicious transmission activity report (STAR) to the Department of Justice (DOJ) within 30 days after detecting a "suspicious transmission" and would require the DOJ to create a database for the public to report suspicious activity.[26]

- On January 26, 2021, Senator Marco Rubio (R-FL) introduced the Adversarial Platform Prevention Act of 2021 (S. 47), which would exempt foreign software providers (e.g., TikTok) from § 230 immunity.[27]

- On February 8, 2021, Senator Mark Warner (D-VA) introduced the Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms (SAFE TECH) Act (S. 299), which would remove immunity if the provider "has accepted payment to make the speech available or . . . created or funded the creation of the speech."[28] The legislation would also convert § 230 immunity into an affirmative defense subject to a preponderance of the evidence standard. Additionally, it would exempt civil rights laws, stalking or harassment laws, wrongful death actions, or human rights violations abroad from § 230 immunity.

- On March 17, 2021, Senator Brian Schatz (D-HI) introduced the Platform Accountability and Consumer Transparency Act (S. 797), which would limit immunity if the provider "has actual knowledge of . . . illegal content or illegal activity" and "does not remove the illegal content or stop the illegal activity" within four days of acquiring knowledge of such content or activities.[29]

- On March 18, 2021, Representative Jim Banks (R-IN) introduced the Stop Shielding Culpable Platforms Act (H.R. 2000), which would remove immunity from platforms that "knowingly" share illegal materials.[30]

- On March 23, 2021, Representative Tom Malinowski (D-NJ) introduced the Protecting Americans from Dangerous Algorithms Act (H.R. 2154), which would remove immunity for providers that use algorithms to rank and promote content, unless the ranking and promoting of such content was "obvious," for example, sorting chronologically or by average user rating.[31]

- On October 15, 2021, Representatives Frank Pallone Jr. (D-NJ), Mike Doyle (D-PA), Jan Schakowsky (D-IL), and Anna Eshoo (D-CA) introduced the Justice Against Malicious Algorithms Act (H.R. 5596), which would eliminate immunity under § 230 when a provider knowingly or recklessly uses an algorithm to recommend content that materially contributes to physical or severe emotional injury.[32]

- In February 2022, Senators Lindsey Graham (R-SC) and Richard Blumenthal (D-CT) reintroduced the EARN IT Act (S. 3538), originally introduced in 2020, which limits immunity for providers who fail to deal with child sexual abuse on their platforms.[33]

That said, there has been some legislation that would repeal § 230 outright, including the Abandoning Online Censorship Act (H.R. 874), introduced on February 5, 2021, by Representative Louie Gohmert (R-TX).[34]

Backlash to the Backlash

Of course, not everyone is a proponent of § 230 reform, let alone a repeal that would likely turn the internet on its head. In addition to the concerns that underpinned § 230 in the first place—that is, that limiting immunity would encourage providers to take a hands-off approach to avoid being tagged with knowledge of their sites' content—critics have cited unintended consequences of past reforms, primarily the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA).[35] FOSTA created a carve-out from § 230 for sites hosting ads for sex trafficking after courts cited § 230 to dismiss claims against sites that allegedly hosted content that promoted trafficked sex workers.[36] Critics say that the law prompted self-censorship—and drove sex trafficking farther underground—because sites deleted any sections that might contain sex trafficking content to avoid having to undertake the effort of determining whether they actually did. They worry that further carve-outs will similarly backfire as providers will remove all manner of lawful, First Amendment–protected content rather than attempting (and inevitably failing) to locate needles in haystacks and hiring legal teams to navigate gray areas between legal and illegal content.[37]

Similarly, attempting to enforce political neutrality would require platforms to aim at a moving target as political views evolve and to attempt to distinguish hyperbolic but in-bounds political campaigning from outright misinformation or hate speech. It is fair to assume that many platforms would just as soon not bother—meaning that misinformation would remain online to avoid accusations of politically motivated removal. Putting aside concerns about potential dangers of such content, hands-off policies could allow political campaigns to commandeer platforms intended to host a dialogue between individuals.

Others have also raised concerns that limitations to § 230 immunity will disproportionately impact smaller providers that are unable to afford the software, staffing, or combination of both that would be required to monitor and remove unlawful content at the speed of the internet. That would undo protections strengthened by case law clarifying that § 230 extends even to single-person operations.[38] Indeed, some Big Tech voices have advocated § 230 reform, including Facebook founder Mark Zuckerberg, who told Congress: "Instead of

being granted immunity, platforms should be required to demonstrate that they have systems in place for identifying unlawful content and removing it."[39]

Moreover, some legislation—particularly the aforementioned EARN IT Act—has been criticized based on the prospect that it could encourage providers to encrypt messages to avoid being tagged with knowledge.[40] That legislation specifically carved out encryption but, even without express language, knowledge-based exemptions could lead to further use of technologies that allow unlawful communications to go undetected.

In addition, there are more practical concerns, including that restricting algorithms and other content-based sorting tools could diminish the navigability and usability of the internet while only incrementally reducing access to unlawful content.[41]

Finally, § 230 reform—especially proposals aimed at neutrality—might limit the ability of providers to "deplatform" speakers whom they believe incite illegality or spread misinformation, or merely post content deemed offensive or undesirable. Such reforms could even threaten sites' ability to enforce their own terms of service. This practice, of course, has made significant headlines, especially the Twitter ban of Trump's account. Courts have continued to reject constitutional challenges to deplatforming, finding that private internet companies are not state actors and that their platforms are not equivalent to a public square under the First Amendment, but legislative limitations on deplatforming and related practices may nonetheless be forthcoming.[42]

Conclusion

The framework established by § 230, despite its imperfections, has facilitated the development of the internet as we know it. The failure of any significant reform to become law, despite years of trying, might signify a reluctance to find out what an internet without § 230 would actually look like. In any event, future proposals and developments must be monitored closely as any significant change will carry important ramifications for online speech, not to mention the navigability and utility of online resources. ◄

Notes

1. 47 U.S.C. § 230.
2. 776 F. Supp. 135, 140–41 (S.D.N.Y. 1991).
3. Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 031063/94, 1995 WL 323710, at *4–5 (N.Y. Sup. Ct. May 24, 1995).
4. 47 U.S.C. § 230(b)(1), (2).
5. *Id.* § 230(b)(3), (4).
6. *Id.* § 230(c)(1).
7. *Id.* § 230(f)(3).
8. Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997).
9. Ben Ezra, Weinstein & Co. v. Am. Online Inc., 206 F.3d 980, 985 (10th Cir. 2000).
10. Doe v. GTE Corp., 347 F.3d 655, 659–60 (7th Cir. 2003).
11. 992 F. Supp. 44, 53 (D.D.C. 1998).
12. 865 A.2d 711, 719–20 (N.J. Super. Ct. App. Div. 2005).
13. Noah v. AOL Time Warner Inc., 261 F. Supp. 2d 532, 538 (E.D. Va. 2003).
14. 934 F.3d 53 (2d Cir. 2019).
15. 521 F.3d 1157 (9th Cir. 2008) (noting that "the company goes by the singular name 'Roommate.com, LLC' but pluralizes its website's URL, www.roommates.com").
16. FTC v. Accusearch, Inc., 570 F.3d 1187, 1190 (10th Cir. 2009).
17. 519 F.3d 666, 668 (7th Cir. 2008).
18. Hill v. StubHub, Inc., 727 S.E.2d 550 (N.C. Ct. App. 2012).
19. 570 F.3d 1096, 1107 (9th Cir. 2009).
20. Doe v. Internet Brands, Inc., 824 F.3d 846, 848 (9th Cir. 2016).
21. Lemon v. Snap, Inc., 995 F.3d 1085 (9th Cir. 2021).
22. Donald J. Trump, Presidential Veto Message to the House of Representatives for H.R. 6395 (Dec. 23, 2020), https://trumpwhitehouse.archives.gov/briefings-statements/presidential-veto-message-house-representatives-h-r-6395.
23. Cristiano Lima, *Biden: Tech's Liability Shield "Should Be Revoked" Immediately*, Politico (Jan. 17, 2020), https://www.politico.com/news/2020/01/17/joe-biden-tech-liability-shield-revoked-facebook-100443.
24. S. 1914, 116th Cong. (2019).
25. S. 27, 117th Cong. (2021).
26. *Id.* § 4.
27. S. 47, 117th Cong. (2021).
28. S. 299, 117th Cong. § 2 (2021).
29. S. 797, 117th Cong. § 6 (2021).
30. H.R. 2000, 117th Cong. § 2 (2021).
31. H.R. 2154, 117th Cong. § 2 (2021).
32. H.R. 5596, 117th Cong. (2021).
33. S. 3538, 117th Cong. (2022).
34. H.R. 874, 117th Cong. (2021).
35. Pub. L. No. 115-164, 132 Stat. 1253 (2018).
36. *See, e.g.*, Doe v. Backpage.com, LLC, 817 F.3d 12, 15 (1st Cir. 2016).
37. *See, e.g.*, *Opinion: The Pitfalls of an Anti-Sex-Trafficking Law Give Congress a Warning*, Wash. Post (June 26, 2021), https://www.washingtonpost.com/opinions/2021/06/26/pitfalls-an-anti-sex-trafficking-law-give-congress-warning.
38. *See, e.g.*, Batzel v. Smith, 333 F.3d 1018, 1031 (9th Cir. 2003).
39. Ryan Tracy, *Facebook's Zuckerberg Proposes Raising Bar for Section 230*, Wall St. J. (Mar. 24, 2021), https://www.wsj.com/articles/facebooks-zuckerberg-proposes-raising-bar-for-section-230-11616610616.
40. *See, e.g.*, Riana Pfefferkorn, *The EARN IT Act Threatens Our Online Freedoms: New Amendments Don't Fix It*, Stan. L. Sch. Ctr. for Internet & Soc'y (July 6, 2020), https://cyberlaw.stanford.edu/blog/2020/07/earn-it-act-threatens-our-online-freedoms-new-amendments-don%E2%80%99t-fix-it.
41. Michal Lavi, *Do Platforms Kill?*, 43 Harv. J.L. & Pub. Pol'y 477 (2020).
42. *See, e.g.*, Prager Univ. v. Google LLC, 951 F.3d 991 (9th Cir. 2020).