Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

Liability for Content Hosts: An Overview of the Communication Decency Act's Section 230

June 6, 2019

Section 230 of the Communications Act of 1934, enacted as part of the Communications Decency Act of 1996 (CDA), broadly protects online service providers like social media companies from being held liable for transmitting or taking down user-generated content. In part because of this broad immunity, social media platforms and other online content hosts have largely operated without outside regulation, resulting in a mostly self-policing industry. However, while the immunity created by Section 230 is significant, it is not absolute. For example, courts have said that if a service provider "passively displays content that is created entirely by third parties," Section 230 immunity will apply; but if the service provider helps to develop the problematic content, it may be subject to liability. Commentators and regulators have questioned in recent years whether Section 230 goes too far in immunizing service providers. In 2018, Congress created a new exception to Section 230 in the Allow States and Victims to Fight Online Sex Trafficking Act of 2017, commonly known as FOSTA. Post-FOSTA, Section 230 immunity will not apply to bar claims alleging violations of certain sex trafficking laws. Some have argued that Congress should further narrow Section 230 immunity—or even repeal it entirely. This Sidebar provides background information on Section 230, reviewing its history, text, and interpretation in the courts.

Legislative History

Section 230 was enacted in early 1996, in the CDA's Section 509, titled "Online Family Empowerment." In part, this provision responded to a 1995 decision issued by a New York state trial court: *Stratton-Oakmont, Inc. v. Prodigy Services Co.* The plaintiffs in that case were an investment banking firm. The firm alleged that Prodigy, an early online service provider, had published a libelous statement that unlawfully accused the firm of committing fraud. Prodigy itself did not write the allegedly defamatory message, but it hosted the message boards where a user posted the statement. The New York court concluded that the company was nonetheless a "publisher" of the alleged libel and therefore subject to liability. The court emphasized that Prodigy exercised "editorial control" over the content posted on its site, actively controlling the content of its message boards through both an "automatic software screening program" and through "Board Leaders" who removed messages that violated Prodigy's guidelines.

Section 230 sought to abrogate *Stratton-Oakmont*. One of the sponsors of the "Online Family Empowerment" provision, Representative Chris Cox, argued on the floor of the House that the ruling

Congressional Research Service
https://crsreports.congress.gov
LSB10306

against Prodigy was "backward." Representative Cox approvingly referenced a different case in which a federal district court had held that CompuServe, another early online service provider, could *not* be held liable for allegedly defamatory statements posted on its message boards. Both Representative Cox and his co-sponsor, then-Representative Ron Wyden, emphasized that they wanted to allow online service providers, working with concerned parents and others, to be able to take down offensive content without exposing themselves to liability. These "Good Samaritan" provisions were intended to ensure that even if online service providers did exercise some limited editorial control over the content posted on their sites, they would not thereby be subject to publisher liability.

Text and Interpretation

In short, Section 230 contains two primary provisions creating immunity from liability. These provisions state that interactive service providers and users may not be held liable for publishing or restricting access to material posted by another information content provider. These two immunity provisions apply broadly in most federal and state civil lawsuits, as well as most state criminal prosecutions. Nonetheless, Section 230 does expressly exempt some suits from its liability shield.

Two terms used in this statute are critical to understanding its scope. Section 230 distinguishes between (1) service providers and (2) content providers (although, as discussed below, any given person or business can be both, depending on the activity). Section 230 defines an "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server." Courts have considered platforms such as Yahoo!, Facebook, Twitter, and Craigslist to be "interactive computer service" providers. By contrast, an "information content provider" is "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."

Section 230(c)(1)

First, Section 230(c)(1) specifies that service providers and users may not "be treated as the publisher or speaker of any information provided by another information content provider." Courts have interpreted this provision broadly, holding that Section 230(c)(1) immunity may apply in any suit in which the plaintiff seeks to hold the provider liable "as the publisher" of another's information, apart from the express exceptions discussed below. Accordingly, Section 230(c)(1) has been applied to bar not only defamation actions like the one at issue in *Stratton-Oakmont*, but also suits alleging, among other things, negligence and violations of state antidiscrimination laws. By contrast, in a decision issued in March 2019, a federal appellate court held that Section 230 did not preempt a Santa Monica ordinance that regulated "home-sharing" and prohibited many types of short term rentals. The court recognized that platforms such as AirBnB might be subject to liability if they violated the ordinance, but nonetheless held that the ordinance did not treat these platforms as publishers. The court noted that platforms would comply with the ordinance by cross-referencing booking transactions against a local property registry, and concluded that the ordinance did not require platforms to police the *content* of third-party listings. In the court's view, monitoring these booking transactions was not equivalent to editorial control or the "'publication' of third-party content."

Section 230(c)(1) immunity may bar a lawsuit if the claim would treat a provider or user of an "interactive computer service" as "the publisher or speaker" of *another*'s content. As courts have held, the converse of this rule is that a service provider can be liable for content that *the service* creates or helps develop. Generally, courts have said that a service's ability to control the content that others post on its website is not enough, in and of itself, to make the service provider a content developer. In some circumstances, a service provider may retain immunity even when it makes small editorial changes to another's content. Some courts have employed a "material contribution" test to determine if Section

230(c)(1) applies, holding that a service provider may be subject to liability if it "materially contribute[d] to the illegality" of the disputed content. Others have said that service providers may be liable if they "specifically encourage[] development of what is offensive about the content."

But ultimately, there are relatively few cases in which courts have held that Section 230(c)(1) immunity is inapplicable because service providers helped to develop the allegedly unlawful content. As one trial court noted, "all but a handful" of the hundreds of reported decisions on this issue have sided with service providers, agreeing that they are entitled to Section 230 immunity. Some have questioned whether this broad application of Section 230 immunity is changing, arguing that in recent years, courts have seemed to take less expansive views of Section 230 immunity. Whether this observation is true remains to be seen. Even if, as an empirical matter, courts have rejected Section 230(c)(1) immunity with increased frequency, this trend might not necessarily be because they are interpreting Section 230 differently. One alternate explanation might be that plaintiffs have gotten better at pleading facts alleging that service providers help develop content, and now bring more meritorious cases. Plaintiffs could also be bringing different types of suits, alleging different causes of actions than in the past.

Section 230(c)(2)

Section 230(c)(2), the second immunity provision, states that interactive service providers and users, as well as services like ad-blockers that provide the "technical means" to filter content online, may not be held liable for voluntarily acting in good faith to restrict access to objectionable material. Consequently, one court described Section 230(c)(2) as applying when a service provider "*does* filter out offensive material," while Section 230(c)(1) applies when providers "*refrain* from filtering or censoring the information on their sites." But as one Section 230 scholar has pointed out, courts sometimes collapse the distinctions between these two provisions and cite Section 230(c)(1) in dismissing suits premised on service providers' decisions to take down certain content. This development could be significant. As noted, Section 230(c)(2) grants immunity only for actions "taken in good faith," while Section 230(c)(1) contains no similar requirement. In this sense, Section 230(c)(2) immunity is narrower than Section 230(c)(1)'s liability shield. At least one trial court has rejected a plaintiff's attempt to claim Section 230(c)(1) immunity over Section 230(c)(2) immunity, saying that where Section 230(c)(2)'s "more specific immunity" covered the disputed actions, the court would not apply Section 230(c)(1) because that would improperly "render[] the good-faith requirement superfluous."

Section 230 Exceptions

Section 230 expressly provides that its immunity provisions will not apply in certain types of lawsuits. Namely, Section 230(e) says that Section 230 will not apply to: (1) federal criminal laws; (2) intellectual property laws; (3) any state law that is "consistent with" Section 230; (4) the Electronic Communications Privacy Act of 1986; and (5) certain civil actions or state prosecutions where the underlying conduct violates specified federal laws prohibiting sex trafficking. Some of these exceptions arise more frequently than others: most significantly, online service providers cannot claim Section 230 as a defense to federal criminal prosecutions or intellectual property claims. The last exception, for certain sex trafficking offenses, was added by FOSTA in 2018.

Considerations for Congress

Courts have generally construed Section 230 to grant internet service providers broad immunity for hosting others' content. Many have claimed that Section 230's immunity provisions were critical to the development of the modern internet, and some continue to defend Section 230's broad scope. But at the same time, a variety of commentators and legislators have questioned whether those immunity provisions

should now be narrowed, given that the internet looks much different today than it did in 1996 when Section 230 was first enacted.

One way for Congress to narrow Section 230's liability shield would be to create additional exceptions, as FOSTA did. As discussed, if a lawsuit does not fall into one of the express exceptions contained in Section 230(e), courts may have to engage in a highly fact-specific inquiry to determine whether Section 230 immunity applies: Section 230(c)(1) immunity will be inapplicable if the provider itself has developed or helped to develop the disputed content, while Section 230(c)(2) immunity may not apply if a service provider's decision to restrict access to content was not made in good faith. For example, prior to FOSTA, courts had split on whether various service providers could be held liable under federal and state laws aimed at sex trafficking. While most courts had concluded that the cases should be dismissed under Section 230, a few courts came to the opposite conclusion, holding that the particular claims before them could proceed because the plaintiffs alleged that the service providers had helped to develop the illegal content published on their sites. Through FOSTA, Congress said that for several sex trafficking offenses, Section 230 immunity would be unavailable regardless of whether or not the service provider materially contributed to the unlawful conduct. (Of course, that does not necessarily mean that the service providers would ultimately be subject to liability in any given lawsuit; it just makes Section 230 unavailable as a defense.) Additional exceptions would similarly obviate these fact-specific inquiries.

Others have argued that Congress should add conditions to Section 230 immunity. For example, some commentators have argued that immunity should be conditioned on transparency about the platforms' content moderation policies and how they are enforced. Germany's Network Enforcement Act requires certain social networks to report on the content they have removed from their platforms. Another option would be a notice-and-takedown system that draws on the model of the Digital Millennium Copyright Act. For a distinct takedown requirement, Congress could also look to the European Union's (EU's) e-Commerce Directive 2000/31/EC. This EU directive is somewhat analogous to Section 230, but it creates immunity for "mere conduit" or "caching" activities. The directive says that "to benefit from a limitation of liability," a service provider must "act expeditiously to remove or to disable access to the information concerned" once the service "obtain[s] actual knowledge or awareness of illegal activities." However, the EU has in recent years considered whether to broaden this immunity shield.

Still others have cautioned that the government should be careful in regulating internet content, expressing free speech concerns. To the extent that Congress favors or disfavors certain types of content, viewpoints, or speakers, the regulation could raise serious First Amendment concerns. In fact, in 1997, the Supreme Court struck down a separate provision of the CDA that made it a crime to send "indecent" or "patently offensive" messages to children, concluding that these prohibitions were too vague and violated the First Amendment. More recently, a number of plaintiffs argued in *Woodhull Freedom Foundation v. United States* that some of the new prohibitions created by FOSTA violate the First Amendment. They claimed that by imposing criminal and civil liability on online services that "promote" or "facilitate" prostitution, Congress unconstitutionally penalized protected speech. The federal district court dismissed the lawsuit on procedural grounds, concluding that the plaintiffs lacked standing. However, in the course of its decision, the court construed the terms "promoting" and "facilitating" more narrowly than the plaintiffs suggested, saying that "FOSTA targets specific acts of illegal prostitution—not the abstract topic of prostitution or sex work." This narrower construction might lessen the First Amendment concerns with the federal laws. This decision has been appealed.

For more information on Section 230 and the regulation of social media, this CRS Report explores in more detail possible First Amendment concerns with the regulation of social media content.

Author Information

Valerie C. Brannon
Legislative Attorney

Disclaimer