Section 230’s Intent Can Guide Online Safety Laws: Legal Insight

Published: Mon Jul 29 04:30:59 EDT 2024

- *Sidley Austin attorneys examine push to change Section 230*
- *Law allows platforms to police content with legal protection*

By Randi Singer and Liz McLean

(Bloomberg Law) --

Whether from Congress or the courts, changes to Section 230 of the Communications Decency Act seem inevitable and will no doubt herald a slew of lawsuits about content moderation. But any proposed changes would benefit from consideration of one of Section 230’s original aims—to give interactive computer services leeway to make their platforms safer.

Congress enacted Section 230 of the Communications Decency Act nearly 30 years ago to encourage interactive computer services such as social media and e-commerce platforms to police themselves. Put simply, these services aren’t liable for content posted by their users if they didn’t develop the content, nor are they liable for removing objectionable material.

Importantly, Section 230 doesn’t provide absolute immunity—it includes carve-outs for federal crimes, intellectual property laws, and certain state, privacy, and sex trafficking laws.

For decades, Section 230 functioned pretty much as intended, encouraging interactive computer services to remove discriminatory and defamatory comments, fraudulent dating profiles, hate speech, and misinformation. Courts typically found Section 230 immunized services when users complain about removed content or terminated accounts.

But in recent years, there has been bipartisan skepticism of Section 230’s continued utility. Cases with increasingly horrific fact patterns—suicide kits, child pornography chatrooms, and sexual predators targeting teenagers—have led to public outcry. Platforms are removing highly politicized and inaccurate posts about vaccines, elections, and social issues for violating terms of service. Critics argue that “big tech” hides behind Section 230 to shirk accountability.

In the face of attacks from both sides—against content that is “censored” and against objectionable content that isn’t removed—potential legislative responses abound. The 30-plus Congressional proposals in the last three years range from limiting Section 230 immunity for certain types of claims or providers, to creating new exceptions, to exposing providers to liability where they have knowledge of harmful content. A congressional subcommittee heard testimony May 22 on a proposal to sunset

Section 230 entirely, risking a "cure" that is significantly worse than the problem it seeks to address.

Supreme Court Sidestep

In the absence of legislation, the US Supreme Court may well decide to act, though it has so far declined to do so. After repeated calls by Justice Clarence Thomas to rein in Section 230 (in dissents to denials of certiorari in *Doe v. Facebook*, *Malwarebytes v. Enigma*, *Biden v. Knight First Amendment Institute*), the justices had the opportunity to reconsider Section 230 last year in *Gonzalez v. Google*.

In a related case with similar facts that was argued at the same time, *Twitter v. Taamneh*, the justices rejected allegations that social media platforms were liable under the Anti-Terrorism Act for an ISIS terrorist attack because plaintiffs failed to allege the platforms substantially assisted the terrorists. The Supreme Court found the platforms' algorithms are agnostic to content—matching any content (regardless of subject) with any user likely to view that content.

Gonzalez v. Google involved similar allegations—ISIS used YouTube, and Google's algorithms surfaced ISIS content. Unlike the defendant in *Taamneh*, Google asserted a Section 230 defense, but the Supreme Court never reached it. Relying on *Taamneh*, the justices in concluded plaintiffs failed to state a claim under the Anti-Terrorism Act and declined to reach Section 230. This dodge left intact the lower court's holding that Section 230 shields algorithm-generated editorial decisions, such as filtering and promoting content, made by platform administrators.

The Supreme Court bypassed the chance to make a Section 230-adjacent argument when considering the constitutionality of two state laws (in Florida and Texas) that restrict social media platforms' ability to "censor" users' speech.

In *Moody v. NetChoice*, the Supreme Court didn't reach the constitutionality of either law, instead remanding both appellate decisions for failing to properly analyze facial constitutional challenges. The majority signaled that social media platforms' content moderation decisions are likely protected by the First Amendment and the state content moderation laws are likely unconstitutional.

The high court's opinion is consistent with the underpinnings of Section 230—the majority in *Moody* noted that if Texas's moderation law was enforced, platforms wouldn't be able to remove disfavored content including Nazi ideology, terrorism, gender violence, and claims of election fraud as they do now. The federal preemption issue raised in the Florida district court wasn't before the justices and remains unresolved.

The day after the Supreme Court issued its *Moody* opinion, Thomas (joined by Justice Neil Gorsuch) issued another dissent to a denial of certiorari, again arguing that the scope of Section 230 immunity

is a question warranting review, so the call to action is still being sounded

Outlook

The costs of defending a lawsuit involving user content without the ability to assert a Section 230 defense at the outset can be crippling, even if a computer service ultimately prevails. That both sides hate Section 230 for vastly different reasons suggests that it is doing exactly what it was meant to do: giving interactive computer services the ability to police their sites with some modicum of legal protection.

While there may well be additional carveouts or tweaks that could be made around the margins, eliminating Section 230 altogether is a mistake. Returning to the pre-Section 230 world would leave interactive computer services with an impossible choice: over-police user content and drastically suppress discourse or stop policing altogether and expose users to a plethora of offensive, explicit, false, and dangerous content. Users are the losers in that world.

This article does not necessarily reflect the opinion of Bloomberg Industry Group, Inc., the publisher of Bloomberg Law and Bloomberg Tax, or its owners.

Author Information

Randi Singer is partner at Sidley Austin focused on copyright, Lanham Act false advertising, and trademark matters.

Liz McLean, a managing associate at Sidley Austin, specializes in intellectual property litigation, representing a variety of clients including social media companies, e-commerce platforms, and biotechnology companies.

Write for Us: Author Guidelines

To contact the editors responsible for this story: Rebecca Baker at rbaker@bloombergindustry.com; Jessie Kokrda Kamens at jkamens@bloomberglaw.com