LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
THURSDAY, OCTOBER 29, 2020

PERSPECTIVE

Pitfalls of proposed amendments to CDA Section 230

By Daniel Rozansky, Cristy Jonelis and Celina Kirchner

Section 230 of the Communications Decency Act has come under fire once again due to Twitter's recent decision to block all access to two articles from the New York Post containing information and images allegedly obtained from Hunter Biden's hacked laptop. This was another in a series of actions Twitter has taken to enforce its terms of use, which began in May when Twitter flagged two tweets by President Donald Trump with the phrase "Get the facts…" and a link to articles providing a different perspective from that put forth by the president. In response, President Trump issued an executive order calling for government agencies to clarify and limit the scope of Section 230 protection. On Sept. 23, the attorney general submitted proposed amendments to Section 230 to Congress, along with a cover letter and a separate explanation of the intended meaning of the proposed amendments.

Section 230 was enacted to immunize online platforms from liability for third-party content posted to their platforms and for the good faith removal of content harmful to children. As currently drafted, Section 230(c)(1) states that: "No provider of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Section 230(c)(2) offers interactive computer service providers immunity from civil liability for "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."

Historically, interactive computer service providers have benefited from courts' broad interpretation of Section 230(c)(1), which has been used to "bar[] lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions — such as deciding whether to publish, withdraw, postpone or alter content." Fed. Trade Comm'n v. LeadClick Media, LLC, 838 F.3d 158, 174-75 (2d Cir. 2016). As such, online platforms such as Twitter, Facebook and Craigslist, have often availed themselves of the protection of Section 230 without having to establish that they restricted access to material "in good faith," as required under subsection (c)(2).

The Department of Justice issued its proposed revisions in part to combat this broad interpretation. The DOJ proposed to amend subsection (c)(1) by clarifying that the protections of that section will no longer apply to an interactive computer service provider's decision to restrict access to material provided by a third party unless the provider removes or limits access to content in "good faith" based on "an objective reasonable belief" that the content "violates its terms of service or use." In other words, only passive publication of third-party content would be granted broad protection under (c)(1).

These proposed amendments to Section 230 increase interactive computer service providers' civil liability exposure. For example, if the proposed amendments had been enacted when Twitter blocked access to the New York Post articles, Twitter likely could not have availed itself of the protection under Section 230(c) due to its inability to satisfy all four factors of 'good faith' restriction.

The DOJ's proposed revisions also limit the protection provided under subsection (c)(2) by removing the "otherwise objectional" category, which the DOJ contends was interpreted so broadly as to render any limitation meaningless. Instead, the DOJ proposes replacing the "otherwise objectionable" language with specific instances of objectionable content — specifically, content that promotes terrorism, "violent extremism," or "self-harm" or that is "unlawful." The DOJ's proposed revisions also remove the subjective standard that currently is contained in subsection (c)(2) by requiring that the provider "have an objectively reasonable belief" that such content is "obscene, lewd, lascivious, filthy, excessively violent, promoting terrorism or violent extremism, harassing, promoting self-harm or unlawful." Interestingly, the proposed amendments do not provide protection from civil liability for restricting access to material that is "untrue." Thus, under the proposed amendment, an interactive computer service provider cannot seek protection under Section 230(c)(2) for restricting access to content based on its own subjective standards of what is appropriate or even to prevent third parties from using the platform to promulgate falsehoods.

The proposed amendments also set forth the requirements an interactive computer service provider must satisfy to demonstrate that a decision to restrict access to content was made in "good faith." An interactive computer service provider will be found to have restricted information in "good faith" when it (1) makes its terms of service or use public, understandable and particularized; (2) abides by those terms of service or use (as well as any other stated content moderation policies); (3) does

not apply its terms of service or use inconsistently (i.e., the same types of content are treated the same way) or restrict information on "deceptive or pretextual grounds"; and (4) provides timely notice to the content provider explaining with particularity the provider's "reasonable factual basis" for restricting access to the content.

These proposed amendments to Section 230 increase interactive computer service providers' civil liability exposure. For example, if the proposed amendments had been enacted when Twitter blocked access to the New York Post articles, Twitter likely could not have availed itself of the protection under Section 230(c) due to its inability to satisfy all four factors of "good faith" restriction. First, Twitter's Hacked Materials Policy was publicly available; however, the New York Post could argue that the policy was not reasonably particularized, as Twitter clarified the policy after removing the articles. Twitter likely satisfies the second element of "good faith," since it restricted access to the articles consistent with its Hacked Materials Policy. Looking to the third element, though, it is likely that the New York Post could find examples of tweets containing hacked materials that were not removed, which would indicate that Twitter does not consistently apply the Hacked Materials Policy. Finally, Twitter waited nearly one day before providing notice to the New York Post of its reason for removing the articles, which arguably would fail to satisfy the fourth requirement to provide "timely notice." Even if Twitter could satisfy all four elements of "good faith," proving this would almost certainly require a jury, and Twitter would incur substantial litigation costs in the process.

As another example, throughout the COVID-19 pandemic, various individuals have used social media platforms to spread what most consider to be scientifically false information, such as claiming that masks are not effective in preventing the spread of the virus or that hydroxychloroquine is a cure for it. Platforms like Twitter took action to remove or moderate this content in order to protect public health. If the DOJ's proposed amendments were in place, Twitter would lose the broad (c)(1) protection currently afforded to it. Instead, if faced with litigation, Twitter would be forced to establish that the removed content objectively violated its terms of use and would need to satisfy all four elements of "good faith" to avoid civil liability. Twitter's decision to remove content, even to protect public health, could lead to civil liability and a substantial evidentiary burden (and corresponding cost) in defending that decision. If Twitter can easily avail itself of Section 230(c) protection so long as it does not restrict access to or flag information as potentially false or misleading, Twitter may allow the proliferation of false information on its platform to avoid a flurry of lawsuits.

The DOJ's proposed revisions also carve-outimmunity for civil actions relating to terrorism, child sex abuse, cyber-stalking and antitrust matters, as well as instances in which the interactive computer service provider knowingly solicits third-party content that would violate federal criminal law. These additional revisions, while important, are not likely to garner the same level of attention as the sweeping proposed revisions to subsection (c).

The value or downside of Section 230 protection remains an ongoing question, but there can be no doubt that the ability of third parties to communicate on the internet, and the right of platforms to moderate that speech, remain critically important. Since the release of these proposed amendments, Federal Communications Commission Chairman Ajit Pai has maintained that the FCC will move forward with rulemaking to interpret the statute and Justice Clarence Thomas called for the U.S. Supreme Court to review its application. See MalwareBytes Inc. v. Enigma Software Group, 2020 DJDAR 11040 (Oct. 13, 2020) (statement of Thomas, J., respecting the denial of certiorari). It remains to be seen whether Congress, the FCC, or the Supreme Court will ultimately change the nature of Section 230 protection and whether those changes will promote the purpose for which the statute was enacted to begin with. ■

Dan Rozansky *is a partner at Stubbs Alderton & Markiles, LLP.*

Cristy Jonelis *is senior counsel in Stubbs Alderton & Markiles, LLP's business litigation practice.*

Celina Kirchner *is an associate in Stubbs Alderton & Markiles, LLP's business litigation practice area.*