ROTHWELL FIGG

Risk Mitigation For Social Media Cos. In Light Of Trump Order

Authored by Steven Lieberman, Christopher Ott, and Jennifer Maisel for Law360
Article
6.22.20

On May 28, President Donald Trump issued an executive order on preventing online censorship targeting the Communications Decency Act, or CDA, titled "Protection for good Samaritan blocking and screening of offensive material."[1]

While there remain serious doubts as to the legality of the order, including the extent to which it is a constitutionally impermissible viewpoint-based regulation of speech, the order makes it clear that the Trump administration will be urging, or even directing, regulators to scrutinize online speech with a view toward attaching consequences to such speech in circumstances in which regulators have, in the past, treated such speech as immune.

For this reason, no matter what the order's legal merits may prove to be, we recommend that companies operating online platforms take this opportunity to review their terms of service agreements and content moderation guidelines. In addition to discussing some areas of focus, we also offer some practical tips for reducing litigation risks.

The CDA Safe Harbor Provisions

The order purports to circumscribe an important but rarely discussed law known as Title 47 of the U.S. Code, Section 230(c).

This law creates safe harbors that protect most online platforms from liability for the words and other communications of third parties who use those online platforms. The safe harbor provisions of Section 230(c) set forth two protections: (1) a publisher protection 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,"[2] and (2) a good Samaritan blocking protection that no provider or user of an interactive computer service shall be held liable on account of "any action voluntarily taken in good faith to restrict

Key Contacts

Steven Lieberman

Jennifer B. Maisel

Related Areas of Practice

Media and Constitutional Law

Technologies

Digital Marketing & Social Media

Media

access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable."[3]

Courts have historically interpreted the publisher provision as shielding service providers from liability for all publication decisions, such as editing, removing or posting information, with respect to content entirely created by third parties.[4]

With decisions issued this year, courts continue to uphold that, with limited exceptions,[5] the publisher provision broadly shields websites and other online computer-based services from liability as a publisher for material posted by others on the service, even when such third-party content is directed to illicit drug sales or promote attacks committed by a terrorist organization.[6]

Thus, the publisher exception remains a vital shield for online platforms that choose to do little about the third-party content that they host.

The good Samaritan provision provides an additional shield for liability for any provider of an interactive computer service that restricts access to content because they consider it obscene or otherwise objectionable.[7]

While Congress' motivating concern for the good Samaritan provision was allowing websites and service operators to restrict access to pornography, the language of the statute is much broader, covering any "excessively violent, harassing or otherwise objectionable" content.[8]

But websites and service operators do not have unfettered discretion to declare online content objectionable, and courts have held that, for example, blocking and filtering decisions driven by anticompetitive animus are not entitled to immunity.[9] Moreover, platforms have an affirmative obligation to block content promoting sex trafficking or terrorism.[10]

Courts over the years have refused to immunize online-based intermediaries under certain scenarios.[11] As stated by one court, "[t]he Communications Decency Act was not meant to create a lawless no-man's-land on the Internet."[12] Courts have, for example, held interactive service providers liable where their own acts, for example, contribute to or induce third parties to express illegal preferences[13] or engage in illegal activities.[14]

The Order

The order came days after Twitter flagged one of Trump's tweets as containing misinformation under Twitter's fact-checking policy. On its surface, Twitter's flagging appears to fall within the good Samaritan safe harbor provision of Section 230(c). However, the order states that "[o]nline platforms are engaging in selective censorship that is harming our national discourse," and references Twitter's decision to "place a warning label on certain tweets that clearly reflects political bias."

To address these perceived biases, the order directs the Commerce Department to petition the Federal Communications Commission to reexamine the scope of the CDA's safe harbor provisions, including the interactions between the publisher and good Samaritan provisions as well as the conditions under which actions restriction access to or availability of material is taken in good faith.[15]

The order has therefore cast aspects of Section 230(c) protection into doubt — at least in the context of administrative action by executive agencies. Putting aside the high likelihood that the order will be given no legal weight by the courts, there are pragmatic steps that online platforms can take to reduce their Section 230(c) litigation risk.

Areas in Which to Reduce Risk

In view of existing and potential limitations in scope of the CDA's safe harbor provisions, we offer a few best practices with respect to terms of service agreements to keep in mind in order to reduce risks from litigation or potentially adverse administrative actions.

Clearly distinguish third-party content from the service provider's content.

The publisher safe harbor provision only protects service providers against claims arising from the publication of content provided by another information content provider.

The terms of service should clearly define information owned and created by a service provider, such as the code, application programming interfaces, and other features and intellectual property owned by the service provider, in addition to information owned by third parties such as users and advertisers.

In publishing or republishing third-party content on a website or app, service providers should be careful that their service at most merely transforms — rather than augments or modifies — such third-party content for publication on an app or service. The greater the lines are blurred between service provider and user-created content, the more risk service providers face in falling outside the scope of Section 230(c)(1).

Clearly disclose your online platform's right to remove or restrict access to third-party content.

A service provider's terms of service should document its right to remove or restrict access to content that may be in violation of the terms of service or any applicable community guidelines.

Consider building in consent to your moderation as a stand-alone aspect of your terms and conditions.

Most people dislike incivility, violence and hate on the online platforms that they frequent. Instead of placing a warning that you retain the right to moderate and ban certain types of speech, consider making this promise to establish a walled garden of civility as a separate feature of your online platform. This will likely reduce risk even beyond changes to the terms and conditions.

Update and adapt internal content moderation policies.

Technological developments will continue to pose new challenges to service operators, whether it is new and more harmful types of malicious code to deep-fake content generated by artificial intelligence technology. In order to ease the burdens of content moderation, consider automated means of screening content and enlisting users to help in the moderation process.

Some content moderation and take-downs will be necessary given the existing limitations in the scope of Section 230, but note that courts have held that notice of the illicit nature of third-party content is insufficient to make such content the service provider's own speech.[16]

Make certain content standards publicly available to set expectations about acceptable postings.

Seizing this opportunity can serve to undercut complaints about partiality. For example, if you make it clear that all uses of a certain expletive will result in removal, it will be harder for a complainant to articulate bias. Bias is not, in and of itself, a Section 230(c) factor. However, because of the order, it would be wise to at least address this risk vector short of litigating Section 230(c) requirements.

Be mindful of industry regulations applicable to your service.

Section 230(c) has several carve outs, including federal criminal law, intellectual property law and electronic communications privacy law.

One court refused to immunize an entity providing services in the home rental space where its service allowed users to target prospective roommates based on race in violation of anti-discrimination laws.[17] Another entity faced potential liability where its advertising platform allowed landlords and real estate brokers to exclude persons of color, families with children, women, people with disabilities and other protected groups from receiving housing ads.[18]

Finally, remember to encourage civil discussion and debate. After all, the remedy for bad speech is more speech, not enforced silence. And be prepared to challenge the order in court in the event that any agency is foolish enough to seek to enforce it.

[1] 47 U.S.C. § 230.

[2] 47 U.S.C. § 230(c)(1).

[3] 47 U.S.C. § 230(c)(2)(A).

[4] See, e.g., Barnes v. Yahoo!, Inc. , 570 F.3d 1096, 1105 (9th Cir. 2009), as amended (Sept. 28, 2009).

[5] Section 230 has a few narrow exceptions, including liability for federal criminal law, intellectual property law, and the Electronic Communications Privacy Act. Additionally, in 2017, Congress passed the Fight Online Sex Trafficking Act ("FOSTA"), codified at 47 U.S.C. § 230(e), providing that Section 230 has "no effect on sex trafficking law" and shall not "be construed to impair or limit" civil claims brought under Section 1595 or criminal charges brought under state law if the underlying conduct would constitute a violation of Sections 1591 or 2421A. Woodhull Freedom Found. v. United States , No. 18-5298, 2020 WL 398625 (D.C. Cir. Jan. 24, 2020).

[6] Knight First Amendment Inst. at Columbia Univ. v. Trump , 953 F.3d 216, 222 (2d Cir. 2020) (noting "Section 230 of the Communications Decency Act explicitly allows social media websites (among others) to filter and censor content posted on their platforms without thereby becoming a 'publisher"); Sen v. Amazon.com, Inc. , 793 F. App'x 626 (9th Cir. 2020) (finding "district court properly granted summary

judgment on Sen's claim for tortious interference with prospective and actual business relations, and interference with an economic advantage, based on the third-party review posted on defendant's website"); Dyroff v. Ultimate Software Grp., Inc. , 934 F.3d 1093 (9th Cir. 2019),cert. denied,No. 19-849, 2020 WL 2515458 (U.S. May 18, 2020) (finding site operator immune under Section 230(c)(1) where service allowed users to register with site anonymously and recommended groups to users, thereby facilitating a fatal drug transaction); Force v. Facebook, Inc. , 934 F.3d 53 (2d Cir. 2019),cert. denied,No. 19-859, 2020 WL 2515485 (U.S. May 18, 2020) (finding Facebook immune under Section 230 against anti-terrorism claims that Hamas, a U.S. designated foreign terrorist organization, used Facebook to post content that encouraged terrorist attacks in Israel); Marshall's Locksmith Serv. Inc. v. Google, LLC , 925 F.3d 1263, 1265 (D.C. Cir. 2019) (finding Google immune from allegations that it "publish[es] the content of scam locksmiths' websites, translat[es] street-address and area-code information on those websites into map pinpoints, and allegedly publish[es] the defendants' own original content").

[7] For example, Section 230(c)(2)(A) could apply to those who developed, even in part, the content in issue or from claims arising not from publishing or speaking, but for actions taken to restrict access to obscene or objectionable content. See, e.g., Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1105 (9th Cir. 2009), as amended(Sept. 28, 2009).

[8] Enigma Software Grp. USA, LLC v. Malwarebytes, Inc. , 946 F.3d 1040, 1047 (9th Cir. 2019).

[9] Id.

[10] Section 230 was amended by the Stop Enabling Sex Traffickers Act (FOSTA-SESTA) in 2018 to require the removal of material violating federal and state sex trafficking laws.

[11] Jeff Kosseff, "The Gradual Erosion of the Law That Shaped the Internet: Section 230's Evolution over Two Decades," 18 Colum. Sci. & Tech. L. Rev. 1, 33-34 (2016).

[12] Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC , 521 F.3d 1157, 1164 (9th Cir. 2008).

[13] Id.

[14] J.S. v. Vill. Voice Media Holdings, L.L.C. , 184 Wash. 2d 95, 103, 359 P.3d 714, 718 (2015) (addressing need "to ascertain whether in fact Backpage designed its posting rules to induce sex trafficking to determine whether Backpage is subject to suit under the CDA").

[15] The order also directs the Federal Trade Commission to evaluate potential anti-conservative bias on social media platforms under its Section 5 authority.

In addition, the order directs that each executive department and agency review and report its Federal spending on advertising and marketing paid to online platforms, and that the Department of Justice review any viewpoint-based speech restrictions imposed by each online platform identified in the report and "assess whether any online platforms are problematic vehicles for government speech due to viewpoint discrimination, deception to consumers, or other bad practices."

This portion of the order is, in our view, particularly vulnerable to invalidation under the First Amendment.

[16] Marshall's Locksmith Serv. Inc. v. Google, LLC , 925 F.3d 1263, 1265 (D.C. Cir. 2019); Universal Commc'n Sys., Inc. v. Lycos, Inc. , 478 F.3d 413, 420 (1st Cir. 2007).

[17] See, e.g., Fair Hous. Counsel of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1163 (9th Cir. 2008).

[18] Nat'l Fair Housing Alliance v. Facebook, Inc., No. 18-cv-2689 (S.D.N.Y., March 2018) (Dkt. 1) (Complaint).

This article was originally published in Law360's Expert Analysis section on June 22, 2020. You may read the article in its entirety below.