Antitrust, Vol. 35, No. 1, Fall 2020.

Section 230: A Law on the Cusp of Change?

BY RYAN MRAZIK AND NATASHA AMLANI

THE COMMUNICATIONS DECENCY ACT, 47 U.S.C. § 230 (CDA), enacted in 1996, establishes that entities known as interactive computer service providers[1] are not liable for (1) communications or content posted by people who use their services, (2) their services' design or structure, or whether and how to allow people to have accounts, and (3) discretionary decisions about removing or restricting access to certain objectionable content. There are exceptions, most notably for violations of federal criminal laws and intellectual property claims, but at bottom, "the law is a simple, common-sense policy: If I go online and post something illegal, I should be the one held responsible, not the message board where I posted it."[2] Further, covered service providers that remove or restrict speech by taking it down, blocking it, or limiting its reach, should not face legal liability for their good faith decisions to take action.

For more than 20 years, the CDA remained basically as it had been enacted. Case law developed its contours, but its protections for covered service providers remained generally intact. Courts largely affirmed the reasons for its enactment and rejected creative pleading theories that, at their core, targeted providers for their actions covered by the CDA. And until recently, it appeared that Congress, regulatory bodies, and courts would not change course.

But times have changed, and a debate about the future of the CDA has erupted into the national consciousness. In August 2019 and May 2020, for example, the *New York Times* published and updated "What is Section 230? Legal Shield for Social Media Is Targeted by Trump" and set out the basic contours of the law and its purpose for the general public.[3] Federal government officials, including President Trump, have targeted Section 230 for potential regulatory intervention and legislative reform, and amending (or even dispensing entirely with) Section 230 even became a talking point during the 2020 campaign season.[4] And at least one Justice of the U.S. Supreme Court has taken note: in October 2020, Justice Clarence Thomas issued an opinion in connection with a denial of certiorari that set out his view that Section 230 immunity had gone beyond its initial and intended scope and should be pared back.[5]

Interested stakeholders are now regularly debating the merits of changes to Section 230 in industry conferences, online, and in the national news media, and courts have been faced with novel theories that seek to circumvent the CDA's protections. Further, the United States is not alone in thinking about how online storage and communications service providers should be regulated, as many other countries and international bodies are proposing changes for how these service providers might be held legally responsible for what people do on their services.

This article provides an overview of these developments, which may lead to dramatic shifts in the legal framework that applies to online services used globally to communicate and share ideas. Although this article does not focus directly on personal privacy rights, the legal protections that apply to covered service providers are key elements of the overarching legal framework that defines the scope of protectable privacy rights online. For example, the right to speak anonymously online, the ability of the government to have speakers censored, and who should be responsible for any range of online conduct, all implicate personal privacy interests.

Executive and Regulatory Proceedings

President Trump squarely targeted Section 230 in May 2020 by issuing his Executive Order on Preventing Online Censorship.[6] The Order includes broad statements about maintaining freedom of expression in the United States, and assertions that online platforms "are engaging in selective censorship," by "'flagging' content as inappropriate, even though it does not violate any terms of service," by "making unannounced and unexplained changes to company policies that have the effect of favoring certain viewpoints," and by "deleting content and entire accounts with no warning, no rationale, and no recourse." These statements in the Order track with public statements by Republican lawmakers who are concerned that online service providers have been politically biased in removing or restricting access to primarily conservative speech.[7]

Ryan Mrazik is a partner in the Commercial Litigation and Privacy and Data Security practices at Perkins Coie LLP in Seattle. Natasha Amlani is an associate in the Commercial Litigation and Privacy and Data Security practices at Perkins Coie LLP in Los Angeles. Ryan and Natasha regularly defend lawsuits brought against service providers that are covered by the Communications Decency Act.

In addition to other directives, the Order set out three regulatory courses of action that would target the protections afforded to covered providers under Section 230.

First, the Order directed the National Telecommunications and Information Administration (NTIA) to petition the Federal Communications Commission for a rulemaking that, if adopted, would severely limit the scope of Section 230. Specifically, the Order states that online service providers that restrict access to or remove content from their platforms should be subject to inquiries about whether their reasons for doing so were pretextual, deceptive, or inconsistent with their terms of service, and whether account holders received adequate notice, a reasoned explanation, and a meaningful opportunity to be heard.

Second, the Order directed the Federal Trade Commission to "consider taking action . . . to prohibit unfair or deceptive acts or practices [that] may include practices by entities covered by section 230 that restrict speech in ways that do not align with those entities' public representations about those practices."

Third, the Order directed the Attorney General to convene state attorneys general to consider state-level action to address the concerns about the scope of Section 230 protections.

The NTIA and FCC process has progressed relatively quickly. The NTIA filed its petition for rulemaking on July 27, 2020. Initial comments on the petition were submitted on September 2, 2020, and replies were submitted by September 17, 2020. There have been almost 20,000 submissions on the docket.[8] Some comments question whether the FCC has the authority to regulate under the CDA and whether the NTIA has the authority to petition the FCC. Other comments state that the NTIA misread the current status of the law and how two distinct provisions of the CDA interact with each other, and that the proposed FCC rulemaking proceeding would lead to bad policy that would disrupt free speech and online commerce.[9] Further comments fall on both sides of the policy debate. At the time this article was written, the comment and reply period for the Petition has closed, and FCC Chairman Ajit Pai issued a statement announcing that the FCC would be moving forward with rulemaking.[10]

Thus far, the FTC and state attorneys general have not publicly disclosed any investigations or actions of the type described in the Order, although some have started to align themselves with President Trump's position.[11] The U.S. Department of Justice did follow on the heels of the Order by issuing a report in June 2020, "Section 230—Nurturing Innovation or Fostering Accountability?" The Report posited that "the time is ripe to realign the scope of Section 230 with the realities of the modern internet," and proposed a number of reforms, including that: (1) service providers not receive legal protection in connection with certain types of content, (2) Section 230 be clarified so that it does not apply to federal antitrust claims, and (3) the contours of the law be adjusted in a way similar to what was proposed in the NTIA petition.[12]

Attorney General William Barr then transmitted draft legislation to Congress on September 23, 2020.[13] The proposal would significantly change Section 230 by: (1) changing the legal analysis that applies to decisions by covered providers regarding restricting access to or availability of content on their services, (2) further specifying the types of content to which covered providers can restrict access without facing liability, (3) exempting additional types of claims from the statutory immunity, and (4) requiring covered providers to implement a notice mechanism whereby the public can notify the provider of material that is unlawful or has been adjudicated as defamatory.

No further legislative or regulatory action has occurred as of yet to effectuate these proposals, and it is unclear how forcefully the Department of Justice may pursue its proposed legislation. The Report and draft legislation indicate that executive branch officials and regulators may seek to drastically rewrite Section 230, steer public debate, and consider investigations and enforcement actions against covered providers.

Legislative Proposals

Current federal legislative proposals focus on two types of changes to the scope of Section 230: (1) compelling online service providers to stop specific conduct, such as use of the internet to find and spread child sexual abuse material (CSAM), advertising practices, and the leasing and rental of real property; and (2) the types of changes proposed in the Order and the Department's proposed legislation, which would limit protections for certain actions by covered service providers to remove or restrict access to content that may be deemed objectionable.

One example of legislation in the first category is the proposed Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT Act).[14] Sponsored by a bipartisan group of legislators, the amended version of the EARN IT Act would change Section 230 by exempting "child exploitation law" from its scope of immunity. Specifically, covered service providers would not be able to assert CDA immunity from civil claims from minors who were victims of CSAM, or from criminal charges or civil lawsuits under state laws regarding advertising, promoting, presenting, distributing, or soliciting CSAM.[15]

The EARN It Act would effectively mirror amendments to the CDA that went into effect in 2018 (the first amendment following enactment of the CDA in 1996), which exempt from Section 230's immunity certain civil lawsuits or state criminal prosecutions regarding sex trafficking. The bills that led to the 2018 amendment—the "Fight Online Sex Trafficking Act" (FOSTA) and "Stop Enabling Sex Trafficking Act" (SESTA)—were widely covered in the press, debated in Congress, and questioned after the fact, in what now looks like a forerunner to the current debates

about further amending Section 230.[16] The EARN IT Act would do effectively the same for CSAM-related conduct, while also laying groundwork for a National Commission on Online Child Sexual Exploitation Prevention that would establish and distribute best practices that covered service providers could adopt to further the law's policy goals. As of the writing of this article, The EARN IT Act is in the Senate, with Democratic Senator Ron Wyden having put a hold on the bill.

The first category also includes legislation to remove CDA immunity for (1) enforcement of state and local laws regarding rental and leasing of real property (presumably to allow enforcement against online marketplaces where people post and arrange for short-term rentals),[17] and (2) entities referred to as "advertising servers," which distribute targeted ads even though an online service provider has told them they do not want the ads to be displayed for users of the service.[18]

The second category includes several proposals, including the "Online Freedom and Viewpoint Diversity Act," primarily from Republican Senator Roger Wicker; the "Stop the Censorship Act of 2020," primarily from Republican Congressman Paul Gosar; the "Stopping Big Tech's Censorship Act" from Republican Senator Kelly Loeffler; the "Limiting Section 230 Immunity to Good Samaritans Act," primarily from Republican Senator Josh Hawley, and the "Ending Support for Internet Censorship Act," also from Senator Hawley.

Each of these bills would circumscribe Section 230 in an attempt to prevent what these Republican lawmakers perceive as politically biased removals or restrictions placed on content by online service providers, similar to what the Department of Justice has proposed. As of the writing of this article, none of these bills has progressed meaningfully, although the Senate Commerce Committee recently heard testimony from the CEOs of major American technology companies regarding Section 230 and these various legislative proposals.

Civil Litigation and Theories

In civil litigation, plaintiffs are exploring theories of liability to avoid the protections afforded by Section 230. A few cases from the last several years illustrate these theories, which courts have rejected in favor of the well-established contours of Section 230's immunity.

That said, Justice Thomas's recent criticism of Section 230 and its immunity could portend a different attitude from the U.S. Supreme Court. On October 13, 2020, in a denial of a petition for a writ of certiorari of a Ninth Circuit case that held Section 230 did not apply, Justice Thomas laid out several areas of Section 230 immunity that are arguably at odds with the text of the statute. He observed that "[c]ourts have long emphasized nontextual arguments when interpreting § 230, leaving questionable precedent in their wake."[19] He specifically called out courts for "failing to distinguish between when a provider is acting as a 'publisher' or a 'distributor' of content, providing immunity to providers for their own content, and extending Section 230 immunity in the context of product defect claims."[20] Although the opinion does not have precedential effect, his statement could further encourage the types of claims described next.

Defective Product Design. Plaintiffs have argued that online service providers should be liable where the design of their product or services allows for impersonation or other dangerous conduct. The most prominent case advancing this theory is *Herrick v. Grindr*,[21] which ultimately reached the Second Circuit Court of Appeals. In the complaint, Matthew Herrick alleged that Grindr, a "hook-up" app, is "defectively designed and manufactured because it lacks safety features to prevent impersonating profiles and other dangerous conduct."[22] Herrick was the victim of a campaign of harassment by an ex-boyfriend, who created profiles on Grindr to impersonate Herrick, to communicate with other people as if the communications were to and from Herrick, and to send people to Herrick's home and workplace. Herrick's legal theory was that he was not seeking to hold Grindr liable for the conduct of his ex-boyfriend but rather for Grindr's own failure to implement safety features or manage its users.

This theory of defective product design did not succeed. The Second Circuit observed that, ultimately, Herrick's claims still "arise from the impersonating content that [his] ex-boyfriend incorporated into profiles he created," and that "his ex-boyfriend's online speech is precisely the basis of his claims that Grindr is defective and dangerous."[23] The Second Circuit, quoting the district court, observed further that "Grindr's alleged lack of safety features is only relevant to Herrick's injury to the extent such features would make it more difficult for his former boyfriend to post impersonating profiles, or easier for Grindr to remove them."[24]

Sex Trafficking Claims. Since the enactment of the Fight Online Sex Trafficking Act, plaintiffs have explored claims against providers whose platforms were used to sexually exploit or traffic victims. In one recent case, a Jane Doe plaintiff sued Kik Interactive, which operates a messaging platform, because adults on the platform used it to contact minors and solicit sexual activity from minors.[25] The plaintiff alleged that Kik had participated in a venture that benefited from and knowingly facilitated Kik account holders using the platform to subject her (and others) to sex trafficking. The case is one of the first to implicate directly the 2018 FOSTA amendments to the CDA, which removed Section 230 immunity for claims of sex trafficking brought under 18 U.S.C. § 1595 against a defendant who knowingly benefits from participating in a sex trafficking venture under 18 U.S.C. § 1591(a).

The district court dismissed the claims under the CDA. After conducting a statutory analysis of the knowledge standards and other provisions of 18 U.S.C. §§ 1595 and 1591, the court concluded that FOSTA and Section 1591 require

"knowing and active participation in sex trafficking by the defendants."[26] This is a high standard. The court observed that "FOSTA did not abrogate CDA immunity for all claims arising from sex trafficking," and ruled that plaintiff's claims that Kik "fail[ed] to enact policies that would have prevented" trafficking did not bring her lawsuit outside the purview of the CDA.[27] This case suggests that plaintiffs who assert claims against service providers whose platforms are used by people to engage in sex trafficking will need to make a significant showing of provider participation to try to hold them liable.

Failure to Warn. Plaintiffs have pursued claims based on a failure to warn theory for a number of years, particularly in the wake of the Ninth Circuit decision in *Doe v. Internet Brands*,[28] on the basis that a covered service provider could be liable for failing to warn account holders of bad actors on their services. Courts have largely rejected this theory, ruling that the claims are based on the content or conduct of third parties who use the services, not the failures of the covered service providers themselves.[29] And even those cases that have accepted that failure to warn claims may not be subject to Section 230 immunity have failed for other reasons, including that covered service providers do not have a duty to account holders to warn them of this type of conduct.[30]

International Developments

Foreign governments and international bodies have also been moving forward with ways to impose liability on online service providers arising primarily from content that people post on their services. These measures would not have direct impact on the scope of Section 230 but may still impact how people communicate online and perhaps also how online service providers operate global platforms for which jurisdictional lines may be difficult to administer.

The U.K.'s Online Harms White Paper. On April 8, 2019, the British Department for Digital, Culture, Media & Sport released the Online Harms White Paper, which proposed a new statutory "duty of care" on companies that provide online services in order to make them "take more responsibility for the safety of their users and tackle harm caused by content or activity on their services."[31] The proposed standard of care is meant to help combat online harms to individuals and harms that undermine the way of life in the U.K. These harms may be caused by content that threatens national security or is terrorist and extremist, as well as a range of other content that relates to child sexual exploitation and abuse, harassment or cyberstalking and bullying, online hate crimes, speech encouraging or assisting suicide, content illegally uploaded from prisons, and other content that could be harmful.

Compliance would be overseen and enforced by an independent regulator with a variety of significant powers, including auditing a provider's compliance with its own terms of service, issuing fines, disrupting the business activities of non-compliant companies, imposing liability on senior management, and imposing measures to block non-compliant services altogether.

The Department for Digital, Culture, Media & Sport and the Home Office published their initial response to public feedback in February 2020, and as of the writing of this article, are in the process of preparing proposed legislation.[32]

European Commission Regulation on Preventing the Dissemination of Terrorism Content Online. On April 17, 2019, the European Parliament adopted its resolution for "Tackling the dissemination of terrorist content online."[33] The resolution would impose several new legal obligations on online hosting service providers with public-facing services with the intent to deter dissemination of online terrorist content. The resolution would impose on service providers a duty to "act in a transparent, diligent, proportionate and non-discriminatory manner in respect of content that they store."[34] In its most operationally onerous requirement, the resolution would require covered entities to remove harmful content within one hour of receiving a removal order from the relevant governmental authority. Penalties for non-compliance would rest with the EU Member States, although the resolution does suggest that "systematic and persistent" failures to comply should be subject to penalties of 4 percent of global turnover in the last business year.

Concerns have been raised, however, that the law would conflict with existing EU legislation and infringe on fundamental human rights. Negotiation regarding the draft text of a revised regulation is currently underway as of the writing of this article.[35]

Australia's Sharing of Abhorrent Violent Material Bill. In April 2019, Australia adopted an amendment to its criminal code called the Sharing of Abhorrent Violent Material Bill, which would create new offenses for certain online companies that fail to report the details of abhorrent violent materials or fail to remove that content.[36] More specifically, the law targets audio, visual, or audio-visual material "that records or streams abhorrent violent conduct engaged in by one or more persons," or "is material that reasonable persons would regard as being, in all the circumstances, offensive . . . ."[37] It also includes acts of terror, murder or attempted murder, torture, rape, and kidnapping. Under the law, providers of internet, content, and hosting services must refer the details of the material to the Australian Federal Police within a reasonable time after becoming aware of its existence.

These examples illustrate the ideas that other countries and international regulatory bodies may consider.[38] The measures are narrowly targeted in some respects but in others are far-reaching: they identify specific types of particularly harmful content (such as CSAM, terrorist content, and hate crimes), but their underlying approach establishes a legislative framework that could easily be adapted to circumscribe other types of online content. As with proposed changes to the CDA in the United States, it remains to be seen whether these proposals will be enacted or implemented and how the changes impact conduct of online service providers and users.

Looking to the Future

Covered service providers might face additional regulations in the future, but there are competing ideas for how that might happen, and indeed, whether it should happen at all. There is a strong contingent of stakeholders who believe no changes are needed and, in fact, argue that proposed changes would be harmful and counterproductive. If the legal calculus does change, the various efforts catalogued above and discussed widely by academics, commentators, and practitioners shed some light on where this debate might be headed.

- **Impose a general standard of care or duty on online service providers.** This idea is set out most fully in the international proposals above but has some traction in U.S. academic literature as well.[39] The Citron and Wittes article recommends keeping Section 230 and its immunity intact but "condition it on a service provider taking reasonable steps to prevent or address unlawful third-party content that it knows about."[40]
- **Target specific types of objectionable content and impose heightened standards on online service providers with regard to those types of content.** This approach is embodied in the U.S. legislative proposals regarding CSAM content and advertising behavior, and is also reflected in the international proposals that call out specific content, such as terrorist material, hate speech, cyberstalking, bullying, and self-harm.
- **Expand civil remedies and state-level enforcement.** This approach, which started with SESTA/FOSTA and is now being considered again with the EARN IT Act, expressly carves out specified claims from Section 230 protection for state attorneys general and civil litigants to assert against covered service providers.
- **Inquire into and regulate service providers' practices.** As set out in the Executive Order and the second type of legislative proposals described above, this approach may require service providers to explain their decisions about content removal or restriction to ensure that they were taken in good faith.

The legislative and regulatory proposals under consideration will continue to prompt policy debates on a range of issues that warrant careful consideration, including the free speech rights of online service providers and people who use their services, the risks of government abuse of potential new content regulation, and the practical burdens on service providers to comply with new legal regulatory obligations. Although these proposals do not focus directly on personal privacy rights, there necessarily is overlap. Given the great and growing importance of online service providers in peoples' everyday lives, the use of the internet for anonymous speech, and the inclusion of compelled access to user data in some legislative proposals, any discussion of proposed CDA amendments will also affect personal privacy rights.

The amount of user activity on interactive computer services and the heightened levels of attention to legal and regulatory issues related to these services shows no sign of slowing. The effects of any changes to legal protections and obligations of these services could be far-reaching. To paraphrase cybersecurity law professor Jeff Kosseff, if Section 230 is the law that "created the Internet,"[41] the proposed changes discussed above, if enacted, could force it to change forever. ■

---

[1] This term is defined broadly as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. § 230(f)(2).

[2] Elliot Harmon, *Changing Section 230 Would Strengthen the Biggest Tech Companies*, N.Y. TIMES (Oct. 16, 2019), https://www.nytimes.com/2019/10/16/opinion/section-230-freedom-speech.html.

[3] https://www.nytimes.com/2020/05/28/business/section-230-internet-speech.html.

[4] *See, e.g.*, Makena Kelly, *Joe Biden Doesn't Like Trump's Twitter Order, But Still Wants To Revoke Section 230*, THE VERGE (May 29, 2020), https://www.theverge.com/2020/5/29/21274812/joe-biden-donald-trump-twitter-facebook-section-230-moderation-revoke.

[5] Malware Bytes v. Enigma Software, Inc., No. 19-1284 (Oct. 13, 2020) (Thomas, J., statement respecting denial of certiorari), https://www.supremecourt.gov/opinions/20pdf/19-1284_869d.pdf.

[6] Donald J. Trump, Executive Order on Preventing Online Censorship (May 28, 2020), https://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/.

[7] *See, e.g.*, Senator Ted Cruz, Letter to The Honorable Ambassador Lighthizer (Nov. 1, 2019), https://www.cruz.senate.gov/files/documents/2019.11.01_USTR%20Sec%20230%20LTR.pdf.

[8] *See* https://www.fcc.gov/ecfs/search/filings?proceedings_name=RM-11862.

[9] *See, e.g.*, Comment of Americans for Prosperity Foundation, In the Matter of the National Telecommunications & Information Administration's Petition to Clarify Provisions of Section 230 of the Communications Act of 1934, as Amended, RM No. 11862 (Sept. 1, 2020), https://americansforprosperityfoundation.org/wp-content/uploads/2020/09/2020.09.02-AFPF-Comment-to-FCC-re-Section-230-Petition-Upload.pdf; Comments of the Center for Democracy & Technology Opposing the National Telecommunications and Information Administration's Petition for Rulemaking, In the Matter of Section 230 of the Communications Act, RM-11862 (Aug. 31, 2020), https://cdt.org/wp-content/uploads/2020/08/CDT-Opposition-to-NTIA-Petition-on-Section-230.pdf.

[10] *See* Statement of Chairman Pai on Section 230 (Oct. 15, 2010), https://docs.fcc.gov/public/attachments/DOC-367567A1.pdf.

[11] *See, e.g.*, Remarks by President Trump in a Discussion with State Attorneys General on Protecting Consumers from Social Media Abuses (Sept. 23, 2020), https://www.whitehouse.gov/briefings-statements/remarks-president-trump-discussion-state-attorneys-general-protecting-consumers-social-media-abuses/.

[12] U.S. Dep't of Justice, Section 230—Nurturing Innovation or Fostering Unaccountability, Key Takeaways and Recommendations (June 2020), https://www.justice.gov/file/1286331/download.

[13] U.S. Dep't of Justice, The Justice Department Unveils Proposed Section 230 Legislation (Sept. 23, 2020), https://www.justice.gov/opa/pr/justice-department-unveils-proposed-section-230-legislation.

[14] 116th Congress, 2d Session, S. 3398 (Mar. 5, 2020).

[15] https://www.judiciary.senate.gov/imo/media/doc/Graham's%20Amendment%20To%20S.3398%20-%20OLL20670.pdf.

[16] *See, e.g.*, David McCabe & Kate Conger, *Stamping Out Online Sex Trafficking May Have Pushed It Underground*, N.Y. TIMES (Dec. 17, 2019), https://www.nytimes.com/2019/12/17/technology/fosta-sex-trafficking-law.html.

[17] Protecting Local Authority and Neighborhoods or the "PLAN Act," H.R. 4322 (Sept. 6, 2019).

[18] Behavioral Advertising Decisions Are Downgrading Services Act, S. 4337 (July 28, 2020).

[19] *Malware Bytes*, *supra* note 5, at 2.

[20] *Id.* at 4.

[21] Herrick v. Grindr, 765 Fed. App'x, 586 (2d Cir. 2019)

[22] *Id.* at 588.

[23] *Id.* at 590.

[24] *Id*.

[25] Doe v. Kik Interactive, No. 20-60702-CIV-SINGHAL, 2020 WL 5156641 (S.D. Fla. Aug. 31, 2020).

[26] *Id*. at *7.

[27] *Id*.

[28] Doe v. Internet Brands, 824 F.3d 846 (9th Cir. 2016).

[29] *See, e.g.*, *id.*

[30] *See, e.g.*, Beckman v. Match, No. 2:13–CV–97 JCM, 2017 WL 1304288 (D. Nev. Mar. 10, 2017).

[31] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

[32] *See* UK Dep't for Digital, Culture, Media & Sport, Online Harms White Paper—Initial consultation response, GOV.UK (Feb. 12, 2020), https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response.

[33] European Parliament, Legislative resolution of 17 Apr. 2019 on the proposal for a regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online P8_(2019)0421, https://www.europarl.europa.eu/doceo/document/TA-8-2019-0421_EN.pdf?redirect.

[34] *Id*. ¶ 12.

[35] *See* Legislative Train Schedule, European Parliament (Sept. 4, 2020), https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-preventing-the-dissemination-of-terrorist-content-online.

[36] Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill 2019, Parliament of Commonwealth of Australia, Senate, https://www.legislation.gov.au/Details/C2019B00074.

[37] *Id*. § 474.31(1).

[38] *See, e.g.*, Broadcasting Authority of Ireland, Revised Audiovisual Media Services Directive (June 24, 2019), https://ec.europa.eu/digital-single-market/en/revision-audiovisual-media-services-directive-avmsd.

[39] Danielle K. Citron & Benjamin Wittes, *The Problem Isn't Just Backpage: Revising Section 230 Immunity*," 2 Geo. L. Tech. Rev. 453 (2018).

[40] *Id*. at 455–56.

[41] Jeff Kosseff, The Twenty-Six Words That Created the Internet (2019).