
October 21, 2020

Competing Congressional and Executive Branch Proposals to Revise Section 230 of the Communications Decency Act

Section 230 of the 1996 Communications Decency Act (“Section 230”) has long afforded online platforms with immunity from certain types of civil action relating to the content of statements posted by the platform’s users. It generally provides that an Internet provider does not become the publisher of a piece of third-party content—and thus subject to certain kinds of liability—simply by hosting or distributing that content. It also provides a safe harbor for companies to take down objectionable content if they act in good faith. Thus, it is often regarded as a cornerstone of social media, shielding online platforms from liability in connection with a variety of claims, ranging from claims of defamation based on users’ posted content¹ to claims based on discrimination in housing.²

The protections that Section 230 has afforded these platforms are now being questioned by members of Congress and the President. Recently, members of Congress in both parties have drafted competing bills to amend Section 230. The President has also weighed in, tweeting that Congress should “REPEAL SECTION 230” and issuing an executive order related to Section 230 in May of this year.³ Democratic Presidential Nominee Joe Biden has also indicated that he is open to revising Section 230.⁴

The future of Section 230’s interpretation in the Supreme Court is also uncertain. On October 13, Justice Thomas concurred in the Supreme Court’s denial of certiorari in a case regarding use of a filtering tool to identify malware threats, which had been dismissed under Section 230. Noting that the Supreme Court had never had occasion to interpret the provision in the 24 years since Congress enacted the statute, at a time when “most of today’s Internet platforms did not exist,”⁵ Justice Thomas wrote separately to “explain why, in an appropriate case,” the Court “should consider whether the text of this increasingly important statute aligns with the current state of immunity enjoyed by Internet platforms.”⁶ He identified lower court decisions that, in his view, read dubious “sweeping immunity” into Section 230 in a way that immunized platforms for their own content,⁷ for editing or altering content,⁸ and for their “own misconduct.”⁹

Earlier this month, the Senate Commerce Committee unanimously approved subpoenas for the CEOs of three of the largest technology companies in the United States (Facebook, Google, and Twitter) to appear for a hearing on Section 230.¹⁰ The CEOs of these companies have agreed to testify before the Committee at the Section 230 Senate hearing, which is currently scheduled for October 28, 2020 and which will also reportedly cover the topics of privacy and “media domination.”¹¹

While there is a bipartisan focus on Section 230, evidenced by nearly a dozen separate proposals to revise Section 230 across the House, Senate, and Executive Branch, the scope of any potential revisions that could

become law remains unclear. None of the current congressional proposals envision a complete repeal of Section 230. Although the Senate Judiciary Committee unanimously reported out the EARN IT Act in July (described in detail below), it has not yet been taken up by the full Senate and the House has not yet indicated an intention to take up a similar version of the bill.

Congress appears unlikely to pass any legislation regarding Section 230 before the upcoming election, particularly as the Senate's hearing with major technology company CEOs is not scheduled to occur until the end of the month; however revisions to Section 230 could be passed during the upcoming lame duck period or early in the next Congress, regardless of the outcome of the election.

Below we summarize Section 230's key provisions as well as the major bills targeting Section 230 that are currently pending in the House or Senate. We also describe the President's recent executive order targeting Section 230 as well as two proposals to revise Section 230 from the Department of Commerce and the Department of Justice that were issued pursuant to the President's executive order.

Section 230's Protections

Currently, Section 230 provides two types of protections for providers of an "interactive computer service" (broadly defined such that it captures most search engines, blogs, social media accounts, etc.). First, Section 230 states that no provider or user of an interactive computer service "shall be treated as the publisher or speaker of any information provided by" the person or entity who created the information itself (*i.e.*, the person who created the content at issue).¹² Courts have interpreted this protection (the "Publisher/Speaker Protection") as a broad federal immunity to any cause of action under most state or federal laws (subject to the limitations within Section 230) that would make a website, social media platform, or internet service provider liable for information created by or originating with a third party.¹³

Second, Section 230 protects interactive computer service providers from civil liability on account of (i) "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" or (ii) "any action taken to enable or make available to [internet content creators] the technical means to restrict access to material described" in clause (i) (the "Objectionable Content Protection").¹⁴ Courts have held this protection to grant immunity to, among other things, anti-malware or other blocking software providers whose products may remove objectionable or potentially hazardous content from, *e.g.*, web searches.¹⁵

Limitation to Section 230 Protections Recently Added by Congress

In April 2018, President Trump signed the Allow States and Victims to Fight Online Sex Trafficking Act ("FOSTA") into law. Among other things, FOSTA added a limitation of Section 230's protections in cases involving certain civil claims and criminal prosecutions under federal laws (and analogous state criminal

laws) that prohibit sex trafficking.¹⁶ According to its sponsors in Congress, FOSTA was intended to allow federal civil suits and state civil suits brought by state attorneys general to proceed against providers of websites that allegedly facilitate or promote sex trafficking.¹⁷ However, courts have generally held that FOSTA does not affect Section 230's protections with respect to state civil claims brought by private litigants.¹⁸

Current Congressional Proposals Regarding Section 230

A number of competing proposals to revise Section 230 have been introduced into the Senate. The Senate Judiciary Committee reported out one bill having bipartisan support regarding Section 230 in July 2020, although the full Senate has not yet taken up that bill. The majority of these proposals have been drafted by Republican senators, although there have also been two bipartisan bills introduced. There has also been at least one bill recently introduced into the House of Representatives by a group of Republican representatives.

While there appears to be general bipartisan interest in potentially revising Section 230 (particularly in the Senate), the different proposed bills vary significantly in scope and intended effects. Some proposals target specific applications of Section 230's protections, particularly in the context of political speech (and these proposals generally do not have bipartisan support). Other proposals are more far-reaching. While none of the current congressional proposals would go so far as to repeal Section 230 as the President has tweeted, several would significantly alter Section 230's protections and impose additional requirements on interactive computer service providers.

Below we summarize these bills and their proposed revisions to Section 230.

The EARN IT Act (Original and Amended Versions)

On March 5, 2020, Republican Senators Lindsey Graham and Josh Hawley and Democratic Senators Richard Blumenthal and Dianne Feinstein introduced a bipartisan bill entitled the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (the "EARN IT Act").¹⁹ The EARN IT Act would create a 19-member "National Commission on Online Child Sexual Exploitation Prevention" (the "Commission") that would be tasked with producing a list of "recommended best practices" related to identifying and reporting online child sexual exploitation. The EARN IT Act would also create a similar limitation of Section 230 immunity in cases related to federal and state child sexual exploitation laws and would add the concept of "earning [Section 230] immunity" with regard to claims under child sexual exploitation laws if an interactive computer service has implemented the best practices adopted by the Commission.

The Commission would consist of the Attorney General, the Secretary of Homeland Security, and the Chairman of the FTC, as well as 16 other members appointed equally by congressional leadership, to include representatives of law enforcement, survivors and victims' services organizations, constitutional law

experts, technical experts, and industry. The best practices to be drafted by the Commission cover a broad variety of topics.²⁰ Once the Commission has released their recommended best practices (within 18 months of the appointment of a majority of the members of the Commission), the EARN IT Act provides for a “fast track” congressional review period prior to such best practices taking effect.

The EARN IT Act would also add a new limitation to Section 230 immunity (similar to the limitation added by FOSTA) in claims relating to civil action rights under, or criminal violations of, federal laws (and analogous state laws) that prohibit the sexual exploitation of children. The EARN IT Act would then add a safe harbor provision preserving Section 230 immunity in civil actions or state criminal prosecutions (but not federal criminal prosecutions) if (i) an officer of the interactive computer service provider certifies to the Attorney General that the interactive computer service provider has implemented and is in compliance with the Commission’s best practices or (ii) the interactive computer service provider has implemented reasonable measures relating to the Commission’s best practices.

After industry participants raised concerns related to the initial draft of the EARN IT Act,²¹ Senator Patrick Leahy proposed an amendment that was ultimately adopted by the Judiciary Committee in July 2020. The amendment added an additional subsection to Section 230 that states that “cybersecurity protections do not give rise to liability.”²² With this addition, the bill would not impose liability if the platform (i) “utilizes full end-to-end encrypted messaging services, device encryption, or other encryption services;” (ii) “does not possess the information necessary to decrypt a communication; or” (iii) “fails to take an action that would otherwise undermine the ability of the provider to offer full end-to-end encrypted messaging services, device encryption, or other encryption services.”

The Senate Judiciary Committee unanimously reported out the amended EARN IT Act on July 2, 2020.²³ To date, the Senate has not taken further action on the EARN IT Act.

The Platform Accountability and Consumer Transparency Act

In June 2020, Democratic Senator Brian Schatz and Republican Senator John Thune introduced a bill titled the “Platform Accountability and Consumer Transparency Act (the “PACT Act”) that would introduce the concept of “intermediary liability” into Section 230.²⁴ The PACT Act also would limit Section 230 immunity in federal civil cases brought by the Attorney General and permit state attorneys general to bring a civil action against an interactive computer service provider in federal court for a violation of federal civil law by the provider on behalf of any affected residents of their state.

Under the “intermediary liability” standard within the PACT Act, Section 230 immunity would not apply to an interactive computer service provider that (i) has knowledge of illegal content being shared or illegal activity occurring on the interactive computer service and (ii) does not remove the illegal content or stop the illegal activity within 24 hours of acquiring that knowledge (“subject to reasonable exceptions based on

concerns about the legitimacy of the notice”).²⁵ “Illegal” content or activity for purposes of the PACT Act is defined as content or activity that has been determined by a federal or state court to be illegal.

The PACT Act would define “knowledge” of the illegal content or activity as a written notification identifying the illegal content or activity with “information reasonably sufficient to permit the provider to locate” the content or account involved, and that also includes: (i) a copy of the order of a federal or state court under which the content or activity was determined to violate federal law or state defamation law; (ii) the complaining party’s contact information; and (iii) a statement made by the complaining party under penalty of perjury that the complaint is accurate and that the content or activity described has been determined by a federal or state court to be illegal.

Separately, the PACT Act would impose additional requirements for interactive computer service providers, including requiring the publication of an acceptable use policy that: (i) “reasonably inform[s] users about the types of content that are allowed on the interactive computer service;” (ii) “explain[s] the steps the provider takes to ensure content complies with the acceptable use policy;” and (iii) “explain[s] the means by which users can notify the provider of potentially policy-violating content, illegal content, or illegal activity” (to include a live company representative accessible via a toll-free number, an email address, and a “complaint system”). The “complaint system” is a system “easily accessible to a user through which the user may submit a complaint in good faith and track the status of the complaint” regarding (i) potentially policy-violating or illegal content or activity or (ii) a decision of the interactive computer service provided to remove content posted by the user. The PACT Act requires interactive computer service providers to remove illegal content or to stop illegal activity within 24 hour hours of receiving notice via the complaint system (subject to the same “reasonable exceptions based on concerns about the legitimacy of the notice”).

If a report is made via the complaint system regarding policy-violating content or activity (as opposed to unlawful content or activity), then the interactive computer service provider would have 14 days after receiving the notice to (i) review the content; (ii) determine whether the content adheres to the acceptable use policy of the provider; and (iii) take appropriate steps. If the provider removes the content that is the target of a complaint, the interactive computer service provider must then “notify the information content provider and complainant of the removal and explain why the content was removed” and have a mechanism in place to permit an appeal of the removal.

The PACT Act would also require that interactive computer service providers publish a “quarterly transparency report” in “a location that is easily accessible to consumers” that details, among other things, the total number of instances in which illegal content, illegal activity, or potentially policy-violating content was flagged internally or due to a user complaint. The report is required to be categorized by: (i) “the category of rule violated;” (ii) “the source of the flag, including government, user, internal automated detection tool, coordination with other interactive computer service providers;” (iii) “the country of the information content provider; and” (iv) any “coordinated campaign, if applicable.” The PACT Act would give the FTC enforcement authority with respect to these additional requirements.

The PACT Act includes exceptions to many of its requirements for “small business providers,” defined as a provider that, during the most recent 24-month period (i) “received fewer than 1,000,000 monthly active users or monthly visitors; and” (ii) “accrued revenue of less than \$25,000,000.”

The Senate Subcommittee on Communications, Technology, Innovation, and the Internet held a hearing on the PACT Act on July 28, 2020, that included representatives from the internet advocacy community.²⁶ To date, the PACT Act has not been passed out of committee.

The Online Freedom and Viewpoint Diversity Act

In September 2020, Senator Graham introduced, along with Republican co-sponsors Senator Roger Wicker and Senator Marsha Blackburn, a separate bill targeting Section 230, titled the Online Freedom and Viewpoint Diversity Act (the “OFVDA”).²⁷ The OFVDA would revise Section 230’s Objectionable Content Protection, which currently affords immunity for interactive computer service providers’ “good faith” actions taken to restrict access to or the availability of material that the provider “considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.” The OFVDA would replace the phrase “considers to be” with “has an objectively reasonable belief is” and would also remove the term “otherwise objectionable” and replace it with “promoting self-harm, promoting terrorism, or unlawful.”²⁸

The OFVDA also would make certain edits to Section 230 to clarify that the definition of “information content provider” includes instances in which a person or entity “editorializes or affirmatively and substantially modifies” content created or developed by another person or entity (with exceptions for minor edits to the formatting, layout, or appearance of such comments). This change appears targeted to remove Section 230 immunity from actions taken by interactive computer service providers that amount to “editorializ[ing] or affirmatively and substantially modif[ying]” content created by others and made available via such interactive computer service providers.

The OFVDA does not currently have any Democratic co-sponsors in the Senate and has not yet been taken up by the Senate Committee on Commerce, Science, and Transportation.

The Online Content Policy Modernization Act

Later in September 2020, Senator Graham introduced a third bill that includes proposed revisions to Section 230’s protections.²⁹ Titled the “Online Content Policy Modernization Act” (the “OCPMA”), the bill largely focuses on a proposed alternative dispute resolution program for copyright small claims. However, Title II of the OCPMA also includes the same substantive changes to Section 230 as the OFVDA. Therefore, if the OCPMA were to be passed and signed into law, its effect with regard to Section 230 would be identical as if the OFVDA were to be passed and signed into law. The OCPMA currently does not have any co-sponsors in the Senate and has not yet been taken up by the Senate Judiciary Committee.

The Ending Support for Internet Censorship Act

In June 2019, Republican Senator Josh Hawley introduced the “Ending Support for Internet Censorship Act” (the “ESICA”), which, if enacted, would provide that Section 230’s protections would only be available to an interactive computer service provider if the provider went through a review process run by the U.S. Federal Trade Commission (“FTC”).³⁰ The ESICA would also amend Section 230 to include a “[r]equirement of politically unbiased content moderation” by interactive computer service providers. In addition, the ESICA would amend Section 230 such that its Publisher/Speaker Protection and Objectionable Content Protection only provide immunity if the FTC certifies that the company does not “moderate information provided by other information content providers in a manner than is biased against a political party, political candidate, or political viewpoint.”³¹ Under the ESICA, once every two years a provider would have to prove “by clear and convincing evidence” to the FTC that the provider does not currently (and within the last two years did not) moderate information in a “politically biased manner.”

“Politically biased moderation” for purposes of the ESICA is defined as a provider’s content moderation practices conducted in a manner that (i) “is designed to negatively affect a political party, political candidate, or political viewpoint; or” (ii) “disproportionately restricts or promotes access to, or the availability of, information from a political party, political candidate, or political viewpoint.” The ESICA would also deny the issuance of a certification to a provider whose employees or officers were found to have made decisions that are “motivated by an intent to negatively affect a political party, political candidate, or political viewpoint.” If an employee took action that the provider later disavowed through specific actions (like publicly displaying the politically biased nature of the information and disciplining the employee), the FTC would not deny immunity certification.

Actions of “[b]usiness necessity” are excluded from the ESICA’s prohibition on politically biased moderation so long as they are “a lawful act that advances the growth, development, or profitability of a company.” However, by definition, a “business necessity” cannot “include any action designed to appeal to, or gain favor from, persons or groups because of their political beliefs, political party membership, or support for political candidates.” ESICA also excludes activities that are not protected under the First Amendment from its prohibition of politically biased moderation.

In order for the FTC to grant an immunity certificate, a majority plus one of the Commissioners of the FTC must vote to approve the issuance of the certificate (with any dissenting opinion made public). The ESICA would require the FTC to review and process immunity certifications within six months of the submission of an application and would permit the FTC to impose a filing fee for such applications. The ESICA would also require the FTC to create a process for public input regarding immunity certification applications.

The ESICA currently does not have any co-sponsors in the Senate.

The Stop the Censorship Act of 2020

In July 2020, Republican Representative Paul Gosar, along with 15 Republican co-sponsors, introduced a bill titled the “Stop the Censorship Act of 2020” (the “SCA”).³² The SCA would revise Section 230’s Objectionable Content Protection by removing the phrase “otherwise objectionable” and replacing it with the phrase “unlawful, or that promotes violence or terrorism.” The SCA would also move a portion of Section 230’s current Objectionable Content Protection, providing immunity for “any action taken to provide users with the option to restrict access to any other material” to a new standalone subsection. Neither the House nor any committee of the House has yet taken up the SCA.

Executive Branch Proposals Regarding Section 230

The Trump Administration has also proposed revisions to Section 230, led by President Trump’s May 2020 executive order targeting alleged online censorship, which instructed the Department of Commerce and Attorney General to draft proposals to revise Section 230. Below we discuss the President’s executive order as well as the proposed revisions to Section 230 from the Department of Commerce and Department of Justice, which have significant substantive overlap.

Executive Order on Preventing Online Censorship

In May 2020, the President issued an “Executive Order on Preventing Online Censorship” (the “Order”) that, among other things, instructed relevant federal departments and agencies to “ensure that their application of [Section 230] properly reflects the narrow purpose of that section and take all appropriate actions in this regard.”³³ Beyond this broad instruction, which did not have immediate legal effect, the Order also required, among other things, (i) the Secretary of Commerce, acting through the National Telecommunications and Information Administration (“NTIA”) to file a petition for rulemaking with the Federal Communications Commission (the “FCC”) requesting that the FCC issue regulations to clarify the scope of Section 230 immunities and what actions that can qualify as being “in good faith” under Section 230; and (ii) the Attorney General to develop a proposal for congressional legislation “that would be useful to promote the policy objections of” the Order.

NTIA Rulemaking Petition to the FCC

On July 27, 2020, NTIA submitted a petition for rulemaking to the FCC regarding Section 230 as required by the Order.³⁴ In the petition, NTIA argues that the FCC should issue regulations to limit Section 230’s Publisher/Speaker Protection (regarding the interactive computer service not being treated as the publisher or speaker of any information provided by another information content provider) such that it would have “no application to any interactive computer service’s decision, agreement, or action to restrict access to or availability of material provided by another information content provider or to bar any information content

provider from using an interactive computer service.” NTIA’s proposed regulations would therefore extend the first immunity only to information posted or uploaded by others to an interactive computer service.

With regard to Section 230’s Objectionable Content Protection, NTIA argues that the FCC should issue regulations that contain “limiting principles” with respect to the scope of immunity afforded to interactive computer services’ decisions to remove or restrict access to content because it is “otherwise objectionable.” NTIA also argues that the true legislative intent with regard to Section 230’s immunity for removing “otherwise objectionable” content was to only grant the immunity for those materials that were objectionable in 1996 (*i.e.*, the year Section 230 was passed) and for which there was already regulation. NTIA states that Congress’ intention in passing Section 230 was “to provide incentives for free markets to emulate” such existing regulations of objectionable materials. NTIA’s proposed regulations would limit Section 230’s Objectionable Content Protection to apply only to the removal of “obscene, violent, or other disturbing matters.”

NTIA also argues that the phrase “good faith” within Section 230 is ambiguous and subjective. To clarify the meaning of “good faith” within Section 230, NTIA’s proposed regulations would define acting in “good faith” to only include situations in which a platform:

- (i) restricts access to or availability of material or bars or refuses service to any person consistent with publicly available terms of service or use that state plainly and with particularity the criteria the interactive computer service employs in its content-moderation practices, including by any partially or fully automated processes, and that are in effect on the date such content is first posted;
- (ii) has an objectively reasonable belief that the material falls within one of the listed categories set forth in [Section 230’s Objectionable Content Protection];
- (iii) does not restrict access to or availability of material on deceptive or pretextual grounds, and does not apply its terms of service or use to restrict access to or availability of material that is similarly situated to material that the interactive computer service intentionally declines to restrict; and
- (iv) supplies the interactive computer service of the material with timely notice describing with particularity the interactive computer service’s reasonable factual basis for the restriction of access and a meaningful opportunity to respond, unless the interactive computer service has an objectively reasonable belief that the content is related to criminal activity or such notice would risk imminent physical harm to others.³⁵

The NTIA petition also advocates for a number of additional regulations to clarify the meaning of the terms within Section 230, including proposed clarifications of the definition of “information content providers” to include “commenting upon” and “editorializing about” content created by others as being outside of the scope of Section 230’s protections. The regulations NTIA proposes would also create an exception to the first Section 230 protection regarding an interactive computer service provider not being “treated as the

publisher or speaker of any information provided by another information content provider” if the interactive computer service provider “actually publishes the content.”

The regulations NTIA proposes would define “actually publish[ing] content” as when an interactive computer service provider “affirmatively solicits or selects to display information or content either manually by the interactive computer service’s personnel or through use of an algorithm or any similar tool pursuant to a reasonably discernible viewpoint or message, without having been prompted to, asked to, or searched for by the user.” This definition would also include situations in which the interactive computer service provider “reviews third-party content already displayed on the Internet and affirmatively vouches for, editorializes, recommends, or promotes such content to other Internet users on the basis of the content’s substance or messages.”

The regulations NTIA proposes would also empower the FCC to impose certain disclosure requirements on internet companies in the same way the FCC requires certain transparency requirements on the providers of broadband internet access.

On October 15, partially in response to the NTIA petition, FCC Chairman Ajit Pai indicated in a statement that the FCC’s “General Counsel has informed [Chairman Pai] that the FCC has the legal authority to interpret Section 230” and therefore the FCC “intend[s] to move forward with a rulemaking to clarify [Section 230’s] meaning.”³⁶ However, it is unclear whether the FCC has authority to issue a binding regulatory interpretation of Section 230 in the way that Chairman Pai’s statement or the NTIA petition suggests.

DOJ Section 230 Report and Proposed Legislation

In June 2020, the U.S. Department of Justice (“DOJ”) published a report titled “Section 230 – Nurturing Innovation or Fostering Unaccountability?” (the “DOJ Report”).³⁷ The DOJ Report states that its basis was a public workshop held in February 2020 with “thought leaders representing diverse viewpoints to discuss Section 230,” written submissions made during the workshop, and “listening sessions” with industry. The DOJ Report proposes a number of changes to Section 230, which generally fall into four categories: (i) incentivizing online platforms to address illicit content; (ii) clarifying federal government civil enforcement capabilities; (iii) promoting competition; and (iv) promoting open disclosure and greater transparency.

The proposed revisions to Section 230 in DOJ’s proposed legislation, which Attorney General Barr submitted to both houses of Congress on September 23, 2020, incorporate the DOJ Report’s four categories of proposed changes.³⁸ Many of DOJ’s proposed edits to Section 230 also are similar to (or in some instances identical to) sections of the proposed FCC regulations drafted by NTIA.

DOJ’s proposed legislation would state that Section 230’s Publisher/Speaker Protection does not apply to situations in which the interactive computer service provider restricts access to or the availability of

material provided by another provider and that, therefore, Section 230 protection in such instances would be governed solely by Section 230's Objectionable Content Protection (as revised in DOJ's proposed legislation). Some courts have applied the Publisher/Speaker Protection to situations in which an interactive computer service provider removes content from a third party or a user or third party's access to the service (e.g., through deletion of a user's account) without reference to the Objectionable Content Protection or its "good faith" test.³⁹

Similar to the proposed regulations from NTIA, DOJ's proposed legislation would add an "objectively reasonable belief" standard to the Objectionable Content Protection and would also remove the term "otherwise objectionable" from this protection. DOJ's proposed legislation adds in other specific types of content that can be restricted or removed, including those that promote "terrorism or violent extremist" or "self-harm" or content that is "unlawful."⁴⁰

DOJ's proposed legislation would also add a "Bad Samaritan Carve-Out" from Section 230 immunity for cases in which an interactive computer service provider was determined to have "acted purposefully with the conscious object to promote, solicit, or facilitate material or activity by another [content provider] that the service provider knew or had reason to believe would violate Federal criminal law." The proposed legislation would also add a carve-out from Section 230 immunity for situations in which a state criminal proceeding or state or federal civil action was brought against an interactive computer service provider in a situation in which a provider had "actual notice" of illegal material or activity on the provider's service and the provider did not do any of the following: (i) "expeditiously remove" or restrict access to such material; (ii) report the material to law enforcement if required by law or as "otherwise necessary to prevent imminent harm; or" (iii) preserve evidence related to the material or activity for at least one year.

The proposed legislation also makes Section 230 immunity unavailable in situations in which an interactive computer service provider fails to remove or restrict access to content "within a reasonable time" after receiving notice from a state or federal court indicating that the material in question is defamatory or unlawful. DOJ's proposed legislation would also require interactive computer service providers to maintain "an easily accessible and apparent mechanism" for users or members of the public to report potentially defamatory or unlawful content.

DOJ's proposed legislation would also expand the current exception to Section 230 immunity regarding the federal government's ability to enforce federal criminal laws to also include the federal government's ability to enforce federal civil laws or regulations. The proposed legislation also expands on FOSTA's exception in cases involving certain civil claims and criminal prosecutions under federal laws (and analogous state laws) that prohibit sex trafficking. DOJ's proposed legislation would include similar exceptions to Section 230 immunity in civil cases involving (i) federal anti-terrorism, cyber-stalking, or antitrust laws, or (ii) state or federal child sex abuse laws.

The proposed legislation would also modify the definition of “information content provider” (*i.e.*, persons who cannot rely on Section 230’s protections), in a manner similar to the proposed regulations from NTIA, to include instances in which an individual or entity “solicits, comments upon, funds, or affirmatively and substantively contributes to, modifies, or alters information provided by another person or entity.” DOJ’s proposed legislation would also add a definition of “good faith” to Section 230 with a four-part test that is virtually identical to the definition of “good faith” included in the proposed FCC regulations from NTIA. In order to be acting in “good faith” under the proposed definition, an interactive computer service provider would be required to (i) have publicly available terms of service that state its content-moderation practices; (ii) restrict content in line with such terms of service; (iii) not restrict access to or availability of content on “deceptive or pretextual grounds;” and (iv) provide timely notice to the person providing the content at issue regarding the provider’s “reasonable factual basis” for the restriction and providing an opportunity for the content provider to respond.

The DOJ’s proposed legislation has not yet been introduced in the Senate or the House.

We will continue to monitor developments related to any potential changes to Section 230, and will provide further updates.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to: _

Meredith Dearborn

+1-650-208-2788

mdearborn@paulweiss.com

Karen L. Dunn

+1-202-223-7308

kdunn@paulweiss.com

William A. Isaacson

+1-202-223-7313

wisaacson@paulweiss.com

Brad S. Karp

+1-212-373-3316

bkarp@paulweiss.com

Claudine Meredith-Goujon

+1-212-373-3239

cmeredithgoujon@paulweiss.com

Jessica E. Phillips

+1-202-223-7338

jphillips@paulweiss.com

Jeannie S. Rhee

+1-202-223-7466

jrhee@paulweiss.com

Kannon K. Shanmugam

+1-202-223-7325

kshanmugam@paulweiss.com

Martha L. Goodman

+1-202-223-7341

mgoodman@paulweiss.com

Associate Joshua R. Thompson contributed to this client memorandum.

¹ See *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997), *cert. denied*, 524 U.S. 937 (1998).

² See *Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 529 F.3d 666 (7th Cir. 2008).

³ Donald Trump (@realDonaldTrump), Twitter (Oct. 6, 2020, 12:08 PM), available [here](#); Executive Order 13925 "Preventing Online Censorship" (May 28, 2020), available [here](#).

⁴ See The New York Times Editorial Board, "Joe Biden Interview," THE NEW YORK TIMES, Jan. 17, 2020, available [here](#).

⁵ *Malwarebytes, Inc. v. Enigma Software Group USA, LLC*, 592 U. S. ____ (2020) (Statement of Justice Thomas respecting the denial of certiorari).

⁶ *Id.* at 2.

⁷ *Id.* at 6.

⁸ *Id.*

⁹ *Id.* at 9.

¹⁰ Press Release, U.S. Senate Committee on Commerce, Science, and Transportation, “Committee Unanimously Approves Authorizations to Subpoena Big Tech CEOs” (Oct. 1, 2020), available [here](#).

¹¹ John Hendel, “Senate Panel Votes to Subpoena CEOs of Google, Facebook, and Twitter,” POLITICO, Oct. 1, 2020, available [here](#).

¹² 47 U.S.C. § 230(c)(1).

¹³ See *Zeran* at 338-339.

¹⁴ 47 U.S.C. § 230(c)(2).

¹⁵ See *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169 (9th Cir. 2009).

¹⁶ 47 U.S.C. § 230(e)(5).

¹⁷ Press Release, Congresswoman Ann Wagner, “Wagner Trafficking Bill Headed to House Floor” (Feb. 21, 2018), available [here](#).

¹⁸ See *J.B. v. G6 Hosp., LLC*, Case No. 19-cv-07848-HSG (N.D. Cal. Aug. 20, 2020).

¹⁹ The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act, S. 3398, 116th Congress, § 6 (2020), available [here](#).

²⁰ *Id.* at § 4(a)(3).

²¹ See e.g. Lily Hay Newman “The EARN IT Act is a Sneak Attack on Encryption” WIRED, Mar. 5, 2020, available [here](#).

²² The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act, S. 3398, 116th Congress, § 5 (2020; amended), available [here](#).

²³ Press Release, Senator Lindsey Graham, “Chairman Graham Applauds Senate Judiciary Committee for Unanimously Approving the EARN It Act” (Jul. 2, 2020), available [here](#).

²⁴ The Platform Accountability and Consumer Transparency Act, S. 4066, 116th Congress (2020), available [here](#).

²⁵ *Id.* at § 6.

²⁶ U.S. Senate Committee on Commerce, Science, and Transportation, “The PACT Act and Section 230: the Impact of the Law that Helped Create the Internet and an Examination of Proposed Reforms for Today’s Online World” (Jul. 28, 2020), available [here](#).

²⁷ The Online Freedom and Viewpoint Diversity Act, S. 4534, 116th Congress (2020), available [here](#).

²⁸ *Id.* at § 2.

²⁹ The Online Content Policy Modernization Act, S. 4632, 116th Congress (2020), available [here](#).

³⁰ The Ending Support for Internet Censorship Act, S. 1914, 116th Congress (2020), available [here](#).

³¹ *Id.* at § 2.

³² The Stop the Censorship Act of 2020, H.R. 7808, 116th Congress (2020), available [here](#).

³³ Executive Order 13925 “Preventing Online Censorship” (May 28, 2020), available [here](#).

³⁴ National Telecommunications and Information Administration, “Petition for Rulemaking of the National Telecommunications and Information Administration” (Jul. 27, 2020), available [here](#).

³⁵ *Id.* at 39-40.

³⁶ Press Release, The Federal Communications Commission, “Statement of Chairman Pai on Section 230,” (Oct. 15, 2020), available [here](#).

³⁷ U.S. Department of Justice, “Section 230 – Nurturing Innovation or Fostering Unaccountability?” (Jun. 17, 2020), available [here](#).

³⁸ U.S. Department of Justice, “Ramseyer Draft Legislative Reforms to Section 230 of the Communications Decency Act” (Sept. 23, 2020), available [here](#).

³⁹ See e.g., *Barnes v. Yahoo!, Inc.*, 570 F.3d, 1096, 1103 (9th Cir. 2009); *Riggs v. Myspace, Inc.*, 444 F. App’x 986 (9th Cir. 2011); *Lancaster v. Alphabet, Inc.*, 2016 WL 3648608 (N.D. Cal. July 8, 2016).

⁴⁰ *Id.* at 1.