U.S. DEPARTMENT OF JUSTICE

Section 230 — Nurturing Innovation or Fostering Unaccountability?

KEY TAKEAWAYS AND RECOMMENDATIONS

June 2020

UNITED STATES DEPARTMENT OF JUSTICE'S REVIEW OF SECTION 230 OF THE COMMUNICATIONS DECENCY ACT OF 1996

As part of its broader review of market-leading online platforms, the U.S. Department of Justice analyzed Section 230 of the Communications Decency Act of 1996, which provides immunity to online platforms from civil liability based on third-party content and for the removal of content in certain circumstances. Congress originally enacted the statute to nurture a nascent industry while also incentivizing online platforms to remove content harmful to children. The combination of significant technological changes since 1996 and the expansive interpretation that courts have given Section 230, however, has left online platforms both immune for a wide array of illicit activity on their services and free to moderate content with little transparency or accountability.

The Department of Justice has concluded that the time is ripe to realign the scope of Section 230 with the realities of the modern internet. Reform is important now more than ever. Every year, more citizens—including young children—are relying on the internet for everyday activities, while online criminal activity continues to grow. We must ensure that the internet is both an open and safe space for our society. Based on engagement with experts, industry, thought leaders, lawmakers, and the public, the Department has identified a set of concrete reform proposals to provide stronger incentives for online platforms to address illicit material on their services, while continuing to foster innovation and free speech.

***

The Department's review of Section 230 arose in the context of our broader review of market-leading online platforms and their practices, announced in July 2019. While competition has been a core part of the Department's review, we also recognize that not all concerns raised about online platforms (including internet-based businesses and social media platforms) fall squarely within the U.S. antitrust laws. Our review has therefore looked broadly at other legal and policy frameworks applicable to online platforms. One key part of that legal landscape is Section 230, which provides immunity to online platforms from civil liability based on third-party content as well as immunity for removal of content in certain circumstances.[1]

Drafted in the early years of internet commerce, Section 230 was enacted in response to a problem that incipient online platforms were facing. In the years leading up to Section 230, courts had held that an online platform that passively hosted third-party content was not liable as a publisher if any of that content was defamatory,[2] but that a platform would be liable as a publisher for all its

[1] The two key operative provisions of Section 230 are: (1) "No 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," and (2) "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 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," 47 U.S.C. § 230(c)(1), (2).

[2] *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135 (S.D.N.Y 1991).

third-party content if it exercised discretion to remove *any* third-party material.[3] Platforms therefore faced a dilemma: They could try to moderate third-party content but risk being held liable for any and all content posted by third parties, or choose not to moderate content to avoid liability but risk having their services overrun with obscene or unlawful content. Congress enacted Section 230 in part to resolve this quandary by providing immunity to online platforms both for third-party content on their services or for removal of certain categories of content. The statute was meant to nurture emerging internet businesses while also incentivizing them to regulate harmful online content.

The internet has changed dramatically in the 25 years since Section 230's enactment in ways that no one, including the drafters of Section 230, could have predicted. Several online platforms have transformed into some of the nation's largest and most valuable companies, and today's online services bear little resemblance to the rudimentary offerings in 1996. Platforms no longer function as simple forums for posting third-party content, but instead use sophisticated algorithms to promote content and connect users. Platforms also now offer an ever-expanding array of services, playing an increasingly essential role in how Americans communicate, access media, engage in commerce, and generally carry on their everyday lives.

These developments have brought enormous benefits to society. But they have also had downsides. Criminals and other wrongdoers are increasingly turning to online platforms to engage in a host of unlawful activities, including child sexual exploitation, selling illicit drugs, cyberstalking, human trafficking, and terrorism. At the same time, courts have interpreted the scope of Section 230 immunity very broadly, diverging from its original purpose. This expansive statutory interpretation, combined with technological developments, has reduced the incentives of online platforms to address illicit activity on their services and, at the same time, left them free to moderate lawful content without transparency or accountability. The time has therefore come to realign the scope of Section 230 with the realities of the modern internet so that it continues to foster innovation and free speech but also provides stronger incentives for online platforms to address illicit material on their services.

Much of the modern debate over Section 230 has been at opposite ends of the spectrum. Many have called for an outright repeal of the statute in light of the changed technological landscape and growing online harms. Others, meanwhile, have insisted that Section 230 be left alone and claimed that any reform will crumble the tech industry. Based on our analysis and external engagement, the Department believes there is productive middle ground and has identified a set of measured, yet concrete proposals that address many of the concerns raised about Section 230.

A reassessment of America's laws governing the internet could not be timelier. Citizens are relying on the internet more than ever for commerce, entertainment, education, employment, and public discourse. School closings in light of the COVID-19 pandemic mean that children are spending more time online, at times unsupervised, while more and more criminal activity is moving online. All of these factors make it imperative that we maintain the internet as an open and safe space.

[3] *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. 1995).

The Section 230 reforms that the Department of Justice identified generally fall into four categories:

1) Incentivizing Online Platforms to Address Illicit Content

The first category of potential reforms is aimed at incentivizing platforms to address the growing amount of illicit content online, while preserving the core of Section 230's immunity for defamation.

a. ***Bad Samaritan Carve-Out.*** First, the Department proposes denying Section 230 immunity to truly bad actors. The title of Section 230's immunity provision—"Protection for 'Good Samaritan' Blocking and Screening of Offensive Material"—makes clear that Section 230 immunity is meant to incentivize and protect responsible online platforms. It therefore makes little sense to immunize from civil liability an online platform that purposefully facilitates or solicits third-party content or activity that would violate federal criminal law.

b. ***Carve-Outs for Child Abuse, Terrorism, and Cyber-Stalking.*** Second, the Department proposes exempting from immunity specific categories of claims that address particularly egregious content, including (1) child exploitation and sexual abuse, (2) terrorism, and (3) cyber-stalking. These targeted carve-outs would halt the over-expansion of Section 230 immunity and enable victims to seek civil redress in causes of action far afield from the original purpose of the statute.

c. ***Case-Specific Carve-Outs for Actual Knowledge or Court Judgments.*** Third, the Department supports reforms to make clear that Section 230 immunity does not apply in a specific case where a platform had actual knowledge or notice that the third party content at issue violated federal criminal law or where the platform was provided with a court judgment that content is unlawful in any respect.

2) Clarifying Federal Government Civil Enforcement Capabilities

A second category of reform would increase the ability of the government to protect citizens from illicit online conduct and activity by making clear that the immunity provided by Section 230 does not apply to civil enforcement by the federal government, which is an important complement to criminal prosecution.

3) Promoting Competition

A third reform proposal is to clarify that federal antitrust claims are not covered by Section 230 immunity. Over time, the avenues for engaging in both online commerce and speech have concentrated in the hands of a few key players. It makes little sense to enable large online platforms (particularly dominant ones) to invoke Section 230 immunity in antitrust cases, where liability is based on harm to competition, not on third-party speech.

4) Promoting Open Discourse and Greater Transparency

A fourth category of potential reforms is intended to clarify the text and original purpose of the statute in order to promote free and open discourse online and encourage greater transparency between platforms and users.

a. ***Replace Vague Terminology in (c)(2).*** First, the Department supports replacing the vague catch-all "otherwise objectionable" language in Section 230 (c)(2) with "unlawful" and "promotes terrorism." This reform would focus the broad blanket immunity for content moderation decisions on the core objective of Section 230—to reduce online content harmful to children—while limiting a platform's ability to remove content arbitrarily or in ways inconsistent with its terms or service simply by deeming it "objectionable."

b. ***Provide Definition of Good Faith.*** Second, the Department proposes adding a statutory definition of "good faith," which would limit immunity for content moderation decisions to those done in accordance with plain and particular terms of service and accompanied by a reasonable explanation, unless such notice would impede law enforcement or risk imminent harm to others. Clarifying the meaning of "good faith" should encourage platforms to be more transparent and accountable to their users, rather than hide behind blanket Section 230 protections.

c. ***Continue to Overrule* Stratton Oakmont *to Avoid the Moderator's Dilemma.*** Third, the Department proposes clarifying that a platform's removal of content pursuant to Section 230 (c)(2) or consistent with its terms of service does not, on its own, render the platform a publisher or speaker for all other content on its service.

* * *

These reforms to Section 230 immunity will incentivize online platforms to police responsibly content that is illegal and exploitive while continuing to encourage a vibrant, open, and competitive internet. These twin objectives of giving online platforms the freedom to grow and innovate while also encouraging them to moderate obscene and unlawful content were the core objectives of Section 230 at the outset. The Department's proposed reforms aim to realize these objectives more fully and clearly so that, in light of the vast technological changes since 1996, Section 230 better serves the interests of the American people.

OVERVIEW OF DEPARTMENT OF JUSTICE'S REVIEW OF SECTION 230

The Department of Justice's review of Section 230 of the Communications Decency Act included a number of different components:

1. ***Public Workshop.*** On February 19, 2020, the Department held a public workshop on Section 230 titled "*Section 230 — Nurturing Innovation or Fostering Unaccountability?*" The workshop gathered experts with diverse views on the benefits and drawbacks of Section 230 and potential reforms. The Attorney General and FBI Director gave opening remarks, followed by three panel discussions with a variety of thought leaders on Section 230, including litigators, academics, victims' representatives, industry representatives, and other experts. The Department of Justice livestreamed the event, *https://www.justice.gov/opa/video/section-230-workshop-nurturing-innovation-or-fostering-unaccountability*, and drafted a written summary.

2. ***Expert Roundtable.*** In the afternoon of February 19, 2020, following the public workshop, the Department hosted a roundtable discussion with additional thought leaders representing diverse viewpoints to discuss Section 230 and potential reforms in further detail. To facilitate a robust dialogue, the afternoon session operated under the Chatham House Rule. The Department drafted a written summary of the roundtable discussion to synthesize the topics discussed, while anonymizing the contributions of the speakers.

3. ***Written Submissions.*** Participants in the morning Workshop and afternoon Roundtable were also invited to submit short written statements with their views on Section 230, which the Department reviewed.

4. ***Industry Listening Sessions.*** Following the Workshop, the Department met individually with companies that had attended the public event or otherwise expressed interest in discussing Section 230. The companies included internet and traditional firms, with diverse businesses and different perspectives on the benefits and harms of Section 230. Meetings were private and confidential to foster frank discussions about how these firms employ Section 230 and their views on potential changes.

The Section 230 Workshop Agenda, Biographies of Participants, Workshop and Roundtable Summary, and Participant Written Submissions are all available at *https://justice.gov/ag/department-justice-s-review-section-230-communications-decency-act-1996*.

DEPARTMENT OF JUSTICE KEY TAKEAWAYS AND AREAS RIPE FOR SECTION 230 REFORM

Based on what we learned from this process, the Department drafted a set of key takeaways, including identifying specific areas that are ripe for reform. The Department's findings are organized into three parts.

Part I highlights core principles to consider in Section 230 reform, including recognition of the benefits of civil immunity in certain circumstances and pitfalls to avoid in reform efforts.

Part II identifies a set of specific areas ripe for reform. The Department's approach attempts to balance the benefits of Section 230 immunity with the need to protect citizens from illicit content and activity online. Rather than repeal the statute entirely at this time, the Department concluded that the best approach would be a measured yet significant recalibration of Section 230 immunity. The reforms are tailored to address specific concerns over particularly harmful content and activity where there is limited speech value, while leaving in place the core immunity for defamation claims based on third-party content. The reforms also aim to clarify and restore the original objective of the statute and give clearer guidance to platforms and courts.

Part III identifies additional areas of potential reform that are still under consideration and would benefit from further analysis and debate. The Department welcomes additional input on whether there are specific reforms that address these topics in a manner consistent with the principles outlined in Part I. Ideas on how these additional areas can be addressed can be sent to **Workshop@usdoj.gov**.

PART I: KEY PRINCIPLES ON SECTION 230 REFORM

1. ***Recognize that Large Tech Platforms Are No Longer Nascent or Fragile.*** Since the enactment of Section 230 almost 25 years ago, the internet and social media ecosystems have grown exponentially. So too have the leading internet and social media companies, which today are some of the most valuable American enterprises. The transformation of a few start-up internet companies into vast transnational enterprises, boasting annual revenues exceeding that of many countries, has raised valid questions of whether those large tech companies still require the blanket immunity Section 230 provided to the nascent internet industry. While it may be imprudent to repeal the immunity entirely, it seems clear that tailored changes to immunity to make the internet a safer place would not unduly burden large tech companies.

2. ***Preserve Competition.*** Section 230 immunity has facilitated the growth of newer tech startups, which have fewer resources to police content and to defend lawsuits than the large tech platforms. At the same time, many are concerned that large online platforms are able to use Section 230 immunity to maintain their dominant positions and avoid regulations or responsibilities that apply to offline competitors, effectively distorting competition. Reforms to Section 230 should aim to preserve and promote competition. Reforms should avoid imposing significant compliance costs on small firms that could raise barriers to entry and entrench dominant platforms and, where possible, should help level the playing field.

3. ***Keep Core Immunity for Defamation To Foster Free Speech.*** One of the key benefits and most frequent uses of Section 230 identified by experts and industry is the protection for online platforms from intermediary liability for defamation based on material posted by third parties on their services. Such immunity is important to avoid chilling free speech online and to promote pro-consumer business models, such as hosting user-generated content and consumer reviews. Platforms generally do not have cost-effective means of evaluating whether a third-party statement is defamatory because they typically do not know if the third-party statement is true or false when made. For example, a review platform generally cannot tell if the statement from a restaurant patron that "the soup was cold" is true or false. Absent immunity, platforms that choose to permit online consumer reviews and third-party content would be likely to remove or censor content whenever someone objects in order to minimize liability risks. Removing the core immunity against defamation claims could imperil certain online business models, particularly for smaller companies. It also could give a heckler's veto to anyone who objects to third-party content, regardless of whether the objection has merit.

4. ***Distinguish between Hosting Defamatory Content and Enabling Criminal Activity.*** While the Department's Section 230 Workshop participants expressed concern about over-censorship if immunity were removed for defamation claims, some participants emphasized the distinction between immunity for defamation-type claims and immunity for enabling dangerous or criminal behavior. Several experts suggested, and the Department generally agrees, that the benefits of immunity do not outweigh the costs when it comes to enabling serious offenses and harms, such as child sexual abuse material and terrorism-related offenses. In such cases, the balance weighs in favor of protecting individuals from harm and giving victims meaningful redress. Where possible, reforms to Section 230 should distinguish between the core immunity for defamation-type torts and claims based on third-party content that facilitates or constitutes federal criminal activity.

PART II: ISSUES RIPE FOR LEGISLATIVE REFORM

Reforms to Better Incentivize Online Platforms to Address Illicit Content

1. Exempting Bad Actors from Blanket Section 230 Immunity

Carve-Out for Bad Actors Who Purposefully Facilitate Criminal Activity or Material

Throughout the Department's discussions, there seemed to be general agreement that online platforms that purposefully promotes, solicits, or facilitates criminal activity by third parties should not receive the benefit of Section 230 immunity, an immunity described in the statute as "Good Samaritan" immunity. A Good Samaritan is someone who stops to help a stranger in need, not someone who endangers the stranger in the first place. To reward bad actors with blanket Section 230 immunity is inconsistent with the purpose of the statute.

Under the current expansive interpretation of Section 230, even websites designed to promote or facilitate illegal conduct can still enjoy the protections of Section 230 immunity. *See, e.g., Daniel v. Armslist, LLC,* 926 N.W.2d 710, 715, 726 (Wis. 2019), *cert. denied.* 140 S.Ct. 562 (2019) (website that facilitated sale of firearm to prohibited person who then murdered wife and two other people, and injured four others was immune under Section 230, despite allegations that website was intentionally designed with the specific purpose of skirting federal firearm laws); *Jones v. Dirty World Entm't Recordings LLC*, 755 F.3d 398, 406 (6th Cir. 2014) (reversing the district court's withholding of Section 230 immunity for "a website owner who intentionally encourages illegal or actionable third-party postings to which he adds his own comments ratifying or adopting the posts").

The Department views an explicit "Bad Samaritan" Carve-Out as necessary to ensure that bad actors do not benefit from Section 230's sweeping immunity at the expense of their victims. If, for example, an online platform purposefully solicits third parties to sell illegal drugs to minors, exchange child sexual abuse material, or otherwise engage in criminal activity on its service, it should not have the ability to turn around and assert blanket Section 230 immunity in all private civil cases.

While experts and industry widely accepted the notion of separating the truly bad actors from the rest, some expressed concerns about a broadly-worded provision that could expose good actors to frivolous litigation. We believe that a few cabining principles would help alleviate this concern.

First, a "Bad Samaritan" Carve-Out should have a heightened *mens rea*, such as "purposefully," under which platforms that accidently or even negligently facilitate unlawful behavior would not lose immunity. Requiring that a platform act purposefully or knowingly would also not impose a burden on platforms to proactively screen all third-party content where there is no indication that the platform

is being used to engage in unlawful activity. At the same time, platforms should not receive immunity where they purposefully promote, solicit, or facilitate the posting of material that the platform knew or had reason to believe would violate federal criminal law.

Second, a "Bad Samaritan" Carve-Out can be limited to platforms that promote, solicit, or facilitate activity or material that the provider knew or should have known would violate *federal criminal law*. This limitation would focus the carve-out on civil and state law cases involving the most egregious categories of content and leave in place the existing blanket immunity for defamation and similar speech torts. While the federal government already has the ability to prosecute platforms for their own criminal activity, such a carve-out would address instances where platforms facilitate criminal behavior by their users as well as provide victims with civil redress.

A "Bad Samaritan" Carve-Out could be enacted instead of, or in addition to, proposals for platforms to earn Section 230 immunity. They are not mutually exclusive. If enacted together with such a proposal, a "Bad Samaritan" Carve-Out would provide a safety net or statutory guardrail on top of a government or private standard-setting process.

Carve-Out for Actors Who Purposefully Blind Themselves and Law Enforcement to Illicit Material

As with the "Bad Samaritan" Carve-Out, it makes little sense to apply "Good Samaritan" immunity to a provider that intentionally designs or operates its services in a way that impairs its ability to identify criminal activity occurring on (or through) its services, or to produce relevant information to government authorities lawfully seeking to enforce criminal laws. A Good Samaritan is not someone who buries his or her head in the sand, or, worse, blinds others who want to help.

One important way to confront the grave and worsening problem of illicit and unlawful material on the internet is to ensure that providers do not design or operate their systems in any manner that results in an inability to identify or access most (if not all) unlawful content. Such designs and operation put our society at risk by: (1) severely eroding a company's ability to detect and respond to illegal content and activity; (2) preventing or seriously inhibiting the timely identification of offenders, as well as the identification and rescue of victims; (3) impeding law enforcement's ability to investigate and prosecute serious crimes; (4) and depriving victims of the evidence necessary to bring private civil cases directly against perpetrators.

We propose making clear that, in order to enjoy the broad immunity of Section 230, an internet platform must respect public safety by ensuring its ability to identify unlawful content or activity occurring on its services. Further, the provider must maintain the ability to assist government authorities to obtain content (i.e., evidence) in a comprehensible, readable, and usable format pursuant to court authorization (or any other lawful basis).

2. Redress for Victims of Terrorism, Child Sex Abuse, and Cyberstalking

Carve-Out for Terrorism Laws

Courts have interpreted Section 230 to apply very broadly, including to block causes of action under civil anti-terrorism laws. *See, e.g.*, *Force v. Facebook*, 934 F.3d 53, 68-72 (2d Cir. 2019); *Fields v. Twitter, Inc.*, 217 F. Supp. 3d 1116, 1118 (N.D Cal. 2016). Given the importance of vigorous criminal and civil enforcement efforts against terrorism, some have proposed that terrorism laws should be explicitly carved out from Section 230 immunity. Immunity for knowingly facilitating terrorist content and activity is far from the core of Section 230, and removing this immunity would not disrupt the internet and social media ecosystems. Moreover, under a traditional tort standard (which would exist absent immunity), platforms would only have to take reasonable steps with respect to the presence of terrorist content; they would not have to achieve perfect success. The Department believes that exempting narrow categories of egregious conduct, like facilitating terrorism, from Section 230's broad immunity strikes the right balance between protecting public safety and national security, on the one hand, and preserving the core of Section 230 immunity, on the other.

Carve-Out for Child Sex Abuse Laws

Many have similarly proposed to carve out from Section 230 immunity civil enforcement of federal child sex abuse laws, and civil and criminal enforcement of state child sex abuse laws. (Federal criminal enforcement of such laws is already carved out.) Immunity for facilitating child sex abuse and child sexual abuse material (CSAM) is not at the core of Section 230, and removing it would not disrupt the internet industry, as shown by the statute's current carve out for human trafficking content. As with the terrorism carve-out, a tort standard would apply in the absence of immunity, so platforms that take reasonable steps to address CSAM and child exploitation still would be protected. The Department supports a tailored carve-out for child sexual exploitation and abuse laws.

Carve-Out for Cyber Stalking

Cyber-enabled stalking is a particularly pernicious and growing threat to victims around the United States. Cyberstalking includes a course of conduct or series of actions by the perpetrator that places the victim in reasonable fear of death or serious bodily injury. Prohibited acts include repeated, unwanted, intrusive, and frightening communications from the perpetrator by phone, e-mail, or other forms of communications, as well as harassment and threats communicated through the Internet, such as via social media sites and applications. Given the importance of criminal and civil enforcement efforts against cyberstalking, the Department would support carving out cyber-stalking from Section 230 immunity, so that victims can seek civil recourse where platforms fail to exercise due care to prevent such illicit and harmful behavior.

3. Notice Liability for Federal Criminal Material and Court Judgments

Case-Specific Carve-Out for Actual Knowledge of Federal Criminal Material

As described above, we believe that platforms that purposefully facilitate egregious illicit activity or material, or are willfully blind to its presence on their services, should be excluded from immunity generally and, thus, should not be entitled to invoke immunity in any case. Additionally, the Department believes that platforms that have actual notice of specific criminal material or activity occurring on their services without taking any action also should not be entitled to immunity in cases arising from such material or activity.

Traditional tort law recognizes several different forms of intermediary liability for publicizing the speech of third parties. *Publishers*, such as newspapers or book publishers, are generally held strictly liable for defamation they publish as if they were the speaker. *Distributors*, such as libraries and newsstands, are held liable only if they knew or should have known the content was unlawful. And *accessories*, such as printing presses, are generally not held liable for defamation.

Section 230 provides that internet services shall not be treated as a "publisher or speaker" of content provided by third parties. Although this language says nothing about distributor liability, courts have interpreted Section 230 broadly to immunize online platforms from liability arising from their publication of third-party content even when the providers had actual notice that content was unlawful and thus could have been held liable at common law as distributors. *See, e.g.*, *Zeran v. America Online Inc.*, 129 F.3d 327 (4th Cir. 1997) (rejecting argument that Section 230 left "distributor liability intact" and holding AOL immune even though it had notice of unlawful nature of the postings); *Universal Commc'n. Sys, Inc. v. Lycos, Inc.*, 478 F.3d 413, 420 (1st Cir. 2007) ("Section 230 immunity applies even after notice of the potentially unlawful nature of the third-party content."). The rationale expressed by courts, and by several participants in the Workshop and Roundtable, is that imposing notice liability on online platforms would chill speech. Some participants suggested that, if platforms were subject to notice liability, they would automatically take down any and all content upon notice without investigation, giving a heckler's veto to anyone who objects to someone else's speech.

When it comes to unlawful content related to federal crimes like child exploitation, drug trafficking, cyber-stalking, or terrorism, however, it is far less clear that we should be concerned about chilling such activity, and instead should be more concerned about halting such dangerous behavior. *See, e.g., M.A. ex rel. P.K. v. Vill. Voice Media Holdings, LLC*, 809 F. Supp. 2d 1041, 1050 (E.D. Mo. 2011) (holding Backpage.com immune under Section 230 from child sex trafficking claims despite allegations that the website was "aware of prior cases of minors being sexually trafficked on its website and based upon the posted ads and photography, no reasonable person could review the postings in the adult categories and deny prostitution was the object of almost each and every ad"). Several participants at the Workshop expressed concern that Section 230 did not provide sufficient incentives for platforms to address such horrendous material, even where they had actual knowledge of its presence and illegality.

While the Department questions whether the text of Section 230 is properly interpreted as immunizing platforms in circumstances in which they knowingly distribute unlawful content, it is clear that a narrower notice liability standard should apply at least in the context of material or activity of third parties that would constitute a federal crime. If a platform has actual notice of specific material or activity that is unlawful under federal criminal law, does not remove the material, report the activity, and preserve related evidence, the platform should not be entitled to immunity for harm resulting from that specific material. This would be a narrow proposal that would not revoke immunity for defamation or similar speech torts, thus avoiding the concern over the heckler's veto. At the same time, this would provide stronger incentives for platforms to address clearly illegal activity and material on their services.

Case-Specific Carve-Out To Encourage Compliance with Court Judgments

Some courts have held that Section 230 provides immunity for online platform even when it fails to take down content that a court has in fact determined to be unlawful. *See, e.g., Hassell v. Bird*, 420 P.3d 776, 789 (Cal. 2018) (holding that Yelp's refusal to comply with a court injunction is protected by Section 230 because its refusal to remove the defamatory material is an "ongoing decision to publish"). Section 230 should be narrowed so as not to apply in actions where a platform has failed to take down content or activity, within a reasonable time, after receiving notice that a court in the United States has adjudicated the content or activity to be unlawful. At the same time, Section 230 should make clear that platforms do have immunity for takedowns consistent with such court orders.

Most online platforms ordinarily comply with court-ordered take-down requests, and such a clarification of the statute would not impose an undue burden. Victims, however, would benefit from having a clear path to remove defamation and other unlawful material from platforms, especially in cases where the underlying poster may not be reachable.

Require Platforms to Provide Users with Mechanisms to Flag Unlawful Content

An online platform is not a Good Samaritan if it sticks its head and the sand and goes out of its way to avoid receiving notice of criminal content on its service. To ensure a platform has the ability to be notified of illegal content, interactive computer services should offer an easily accessible and apparent mechanism for users to give notice to providers so they have an opportunity to review and remove it where appropriate. Otherwise, there is a risk that a platform might attempt to avoid receiving actual notice by making it impossible or difficult for users to flag illicit material.

Under current case law interpreting Section 230, courts have held having a mechanism for users to alert platforms of illegal activity is a voluntary precaution that Section 230 permits but does not require. *See, e.g.*, *Daniel v. Armslist*, *LLC*, 926 N.W. 2d 710, 722 (Wis. 2019). The Department supports a provision requiring an interactive computer service to have easy and apparent mechanism for users to flag unlawful content in order to benefit from Section 230 immunity. The mechanism should be reasonable based on the size and nature of the interactive computer service.

Clarifying Federal Government Civil Enforcement Capabilities

Currently, Section 230 expressly precludes immunity in federal criminal enforcement actions, *see* § 230(e)(1), but some have suggested that Section 230 immunity may lie against the federal government in civil enforcement matters. Recently, the federal government has seen an uptick in instances in which Section 230 immunity is raised in negotiations over federal civil litigation, or is invoked as a defense in federal civil enforcement actions. In discussions the Department held with thought leaders, industry representatives, and legal experts, there was wide agreement that Section 230 should not apply to suits brought by the federal government. Indeed, many were surprised to hear that this was even an issue the government was facing.

Civil enforcement is an important complement to the federal government's criminal prosecutions. Civil actions by the federal government also would not raise the concern of a flood of private damages litigation over state law claims of defamation that Section 230 in part sought to address. The Department therefore believes that Section 230 should be amended to make clear that its immunity does not apply in any case brought by the federal government, whether criminal or civil.

Reform to Promote Competition

A concern that many have raised in the context of Section 230 and more broadly is the increased size and power of a small handful of online platforms. This is relevant in the Section 230 discussion for those citizens who want safer online spaces, for those whose speech has been banned or restricted by these platforms, and for upstart businesses trying to compete against these platforms. Over time, the avenues for sharing information and engaging in discourse with a large number of individuals have concentrated in the hands of a few key players. Further, the big tech platforms of today often monetize through targeted advertising and related businesses, rather than charging users. Thus, their financial incentives in content distribution may not always align with what is best for an individual user.

Antitrust law prohibits dominant firms from engaging in anticompetitive conduct that harms competition. In some cases, online platforms have argued that Section 230 creates an immunity from antitrust claims. *See, e.g.*, *Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1050 (9th Cir. 2019) (rejecting Malwarebytes's contention that it was immune from liability under Section 230 "regardless of any anticompetitive motives") (cert pending).

Immunity against antitrust claims, however, was not part of the core objective of Section 230. In an antitrust case, the key question is whether a defendant is engaging in conduct that harms competition. Such claims are not based on third-party speech, nor do they focus on whether the platform is a publisher or speaker.

Given this, and the existing market dynamics, it is important to ensure that Section 230 is not used as a tool to block antitrust claims aimed at promoting and preserving competition. Interpreting Section 230 based on its text and original purpose does not appear to preclude federal antitrust claims. However, the Department believes it would be useful to create an explicit legislative carve-out from Section 230 for claims under the federal antitrust laws. Until then, there is a risk that defendants will continue to try to use Section 230 creatively to block antitrust actions.

Reforms that Promote Open Discourse and Greater Transparency

1. Replace Vague Language to Address Moderation Beyond Section 230

Currently, Section 230(c)(2) immunizes platforms from liability related to restricting access to, or the availability of, material that the platforms consider "obscene, lewd, lascivious, filthy, excessively violent, harassing, or *otherwise objectionable*." 47 U.S.C. § 230(c)(2)(A) (emphasis added). Courts have disagreed over how much discretion platforms have to decide what is "otherwise objectionable." Some construe the phrase to confer virtually unlimited discretion on platforms to remove any content they object to, for whatever reason. *See, e.g.*, *PC Drivers Headquarters, LP v. Malwarebytes Inc.*, 371 F. Supp. 3d 652, 662 (N.D. Cal. 2019); *Langdon v. Google, Inc.*, 474 F. Supp. 2d 622, 631 (D. Del. 2007). Others counter that such unconstrained discretion would be inconsistent with the policy goals Congress set forth in Section 230. *See, e.g.*, *Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1049-51 (9th Cir. 2019). Those goals include "preserv[ing] the vibrant and competitive free market that presently exists for the Internet," 47 U.S.C. § 230(b)(2), and maintaining the Internet as "a forum for a true diversity of political discourse," *id.* § 230(a)(3).

Unconstrained discretion is particularly concerning in the hands of the biggest platforms, which today effectively own and operate digital public squares. This is even more salient today where social distancing requirements have driven more speech and interaction online. The vagueness of the term "otherwise objectionable" risks giving every platform a free pass for removing any and all speech that it dislikes, without any potential for recourse by the user. Therefore, to bring the immunity conferred by (c)(2) more in line with the interests Congress identified in the original CDA, the Department proposes deleting the vague phrase "otherwise objectionable," while adding a new immunity for moderation of material the platform believes, in good faith, violates federal law or promotes violence or terrorism. By both narrowing and expanding 230(c)(2) in these ways, the proposals strike a more appropriate balance between promoting an open, vibrant Internet and preserving platforms' discretion to restrict obscene and unlawful content.

To be clear, the Department's proposal would not leave platforms unable to moderate content on their services. Nor does removal of blanket immunity itself impose liability for content moderation decisions. Online platforms are often protected by their terms of service when removing content that violates the platform's rules, whether or not that content falls into the categories of (c)(2). Therefore, removing Section 230 immunity from certain content moderation decisions means that platforms must rely on—and abide by—their terms of service. In our view, incentivizing platforms to be more transparent and clear in their terms of services, including with respect to content removal decisions, will ultimately benefit users.

2. Provide Definition of Good Faith

Under subsection (c)(2), platforms must act in "good faith" to receive immunity related to content-moderation decisions. Several experts have raised the concern, however, that platforms are ignoring this "good faith" requirement and censoring material in deceptive or pretextual ways.

To address this problem, the Department suggests providing a definition of what constitutes "good faith." To restrict access to particular content in "good faith," a platform should be required to meet four criteria. First, it must have publicly available terms of service or use that state plainly and with particularity the criteria the platform will employ in its content-moderation practices. Second, any restrictions of access must be consistent with those terms of service or use and with any official representations regarding the platform's content-moderation policies. Third, any restrictions of access must be based on an objectively reasonable belief that the content falls within one of the categories set forth in subsection (c)(2)(A). And fourth, the platform must supply the provider of the content with a timely notice explaining with particularity the factual basis for the restriction of access, unless the provider reasonably believes that the content relates to criminal activity or notice would risk imminent harm to others. These requirements aim to encourage greater transparency in platforms' content-moderation decisions.

3. Continue to Overrule *Stratton Oakmont* to Avoid the Moderator's Dilemma

Congress enacted Section 230 in part to overrule the *Stratton Oakmont* decision, in which a platform was held to be responsible for all content on its service because it chose to moderate some content on its service. *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. 1995). Workshop participants expressed concern that reforms to Section 230 might reintroduce the "Moderator's Dilemma," forcing a platform to choose between moderating content (and therefore exposing itself to liability for all other user-generated content), or not moderating at all (and therefore hosting whatever content, however repugnant, that users post).

The Department agrees that it is important to avoid the Moderator's Dilemma and supports adding a provision to make clear that a platform's decision to moderate content either under (c)(2) or consistent with its terms of service does not automatically render it a publisher or speaker for all other content on its service.

Although a takedown decision either under (c)(2)(A) or consistent with a platform's terms of service does not render an online platform a publisher or speaker for all other content, those actions are treated differently with respect to the statutory immunity. A takedown decision pursuant to (c)(2)(A) is immune from civil liability under Section 230. A platform's removal or restriction of content outside of (c)(2)(A) is not entitled to Section 230 immunity—under either (c)(1) or (c)(2)—even if consistent with the platform's terms of service.

PART III: IDEAS UNDER FURTHER CONSIDERATION

1. ***Distinguish Between Different Types of Internet Services.*** A number of experts and industry participants highlighted the distinction between different types of interactive computer services. Some services, like internet service providers, primarily serve as the "pipes" for content to flow through and have a more limited ability to detect and report criminal activity. Section 230's current definition of "interactive computer services" may also be interpreted to include collateral services that are not user-facing and do not themselves host user content. Many of the proposals for reform appear most concerned with platforms that solicit and curate user-generated content—what some call "digital curators." There is an open question on whether and how to vary immunity and responsibility for the different types of services, especially when technology continues to change.

2. ***Distinguish Between First-Party and Third-Party Speech.*** Several Workshop participants noted a distinction between when platforms are engaging in their own speech and when they are hosting third-party speech. Section 230 does not grant immunity to online platforms from claims arising from information they (rather than a third-party) provide, or from conduct or design decisions. If a platform is speaking in its own right – or if it edits or contributes to a third-party post – then it has become an "information content provider" and unable to seek the protection of Section 230 immunity. See § 230(f)(3). The Section 230 analysis of when a platform becomes an "information content provider," however, becomes harder with industry's use of proprietary algorithms and other technologies, which blur the line between first and third-party speech.

3. ***Address Republication Liability.*** Relatedly, some Workshop participants expressed a view that Section 230 should not immunize platforms for ratification, republication, or amplification of unlawful speech. As one participant noted, "freedom of speech is not freedom of reach." The question is how to define republication where algorithms and technology could be seen as "republishing" or "amplifying" almost all speech on the service. While there may be a way to distinguish where a platform actively promotes speech on the basis of its substance (e.g., featured story of the day or sponsored content), this distinction should be carefully considered and defined.

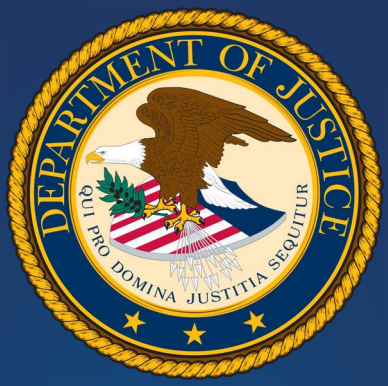
4. ***Sunsetting May be Appropriate.*** Given how quickly technology changes, some have expressed the view that it may be appropriate to sunset Section 230 immunity so that future legislators must revisit whether technological changes warrant changes to the scope of Section 230 or whether the immunity is no longer necessary.

5. ***Transparency Reporting Requirements.*** To foster greater transparency in how platforms enforce their content moderation policies, some experts have proposed requiring large platforms to regularly disclose data on the enforcement of their content moderation policies in order to receive or keep Section 230 immunity. Such disclosure would serve multiple important aims.

   First, it would enable members of the public to identify best practices related to restricting harmful content. For example, the disclosures could provide data on how aggressively platforms are enforcing their policies, how they are identifying improper material, and how long it takes them to remove such material. Scholars, policymakers, and other platforms could use such information to improve content moderation practices and better protect against the range of unlawful material that appears online.

   Second, disclosure of enforcement data would address concerns that large platforms discriminate against particular viewpoints in enforcing their content moderation policies. Currently, platforms have no obligation to disclose data that would enable third-parties to evaluate whether such bias claims are true. As many experts agreed, access to robust enforcement data would enable policymakers and the public to evaluate whether platforms are enforcing content moderation policies even-handedly across different political viewpoints and communities.

   Enforcement data may help to alleviate suspicion of platforms if, as some experts claim, complaints of bias simply reflect that, given the scale of large platforms, there are many anecdotal examples that individuals can point to as evidence of bias but that in reality are not representative of overall content moderation decisions. Alternatively, enforcement data may help inform consumer choices or policy solutions if they reveal that claims of bias are well-founded. Either way, public disclosure of robust enforcement data appears useful to ensuring that the internet remains, in the words of the CDA, "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity." 47 U.S.C. § 230(a)(3).


DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR