Written Testimony

HEARING BEFORE THE UNITED STATES SENATE

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION'S SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY, INNOVATION

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

July 28, 2020
Testimony of Elizabeth Banker
Deputy General Counsel, Internet Association

Chairman Thune, Ranking Member Schatz, and members of the Subcommittee, thank you for inviting me to testify at this important hearing today. My name is Elizabeth Banker, and I am Deputy General Counsel of Internet Association.

Internet Association is grateful for the opportunity to appear before this Subcommittee to discuss Section 230 — the foundational law that has fostered the development and growth of the variety of online services that consumers consider the best of the internet. We appreciate the Subcommittee's thoughtful approach to understanding the history and purpose of Section 230, and I hope my testimony will assist in your efforts.

IA is the only trade association that exclusively represents leading global internet companies on matters of public policy. IA's mission is to foster innovation, promote economic growth, and empower people through the free and open internet. IA believes the internet creates unprecedented benefits for society, and as the voice of the world's leading internet companies, IA works to ensure policymakers and other stakeholders understand these benefits.

Section 230 plays a critical role in empowering companies to offer innovative services and set and enforce policies regarding the use of those services. IA hopes, through our testimony, to explain: 1) how Section 230 enables our members' services by allowing them to take action against harmful activity when they find it; 2) how the law strikes a careful balance by barring certain types of lawsuits and encouraging moderation; 3) the role of the First Amendment in this debate; and 4) considerations for policymakers looking at possible amendments to Section 230 including IA's preliminary thoughts on the PACT Act. This testimony also provides new research, based on our analysis of more than 500 court decisions involving Section 230, that sheds light on the wide variety of parties using the law, how the law affects litigation, and how courts apply it.

Many of the things people consider to be the "best of internet" are possible because of Section 230. IA's research shows that consumers value hearing from other consumers about their experiences before making major purchases, booking travel, and ordering a ride-share.[1] Consumers check online reviews more frequently than recommendations from experts or friends. Section 230 allows users to access and share a wide range of information, opinions, and experiences. This type of sharing is at the core of many IA members' services and is what makes them enjoyable, useful, and engaging for their users. It is difficult to imagine a world where all of that would be possible if, for example, a travel site could be held legally responsible for every word in every review it hosts.

IA member companies recognize that in order to realize the full benefits of the internet, it is critical that they take action to prevent and respond to harmful online activities. This is essential to building and maintaining both user and public trust. Today's world, where we grapple with a global pandemic and a social justice movement that is a reckoning with lives lost to systemic discrimination, has shown both the tangible benefits of online services and the critical role providers play in ensuring that their services are not undermined and misused in ways that threaten individual lives or the public good.

IA members have played an essential role in helping society transition into today's "new normal." Their services allow us to stay connected to loved ones, order takeout to support local restaurants, conduct doctors' appointments via telehealth services, and even work from home through video conferences.

While IA's members recognize that their platforms always have room for improvement, they are consistently working to find ways to make their services safer — whether by highlighting authoritative sources of accurate information about COVID-19 and addressing dangerous misinformation, or by working to make underrepresented and marginalized groups feel that they have a safe place to express themselves. Many of our members have made commitments as a result of recent events to do more, and IA as an organization is also actively working to support these efforts. IA has centralized and detailed member company efforts in response to COVID-19 as a resource for the public and policymakers.[2] As part of its commitment to social justice, IA is building on the work in its 2019 Diversity & Inclusion Benchmark Report; helping underrepresented groups find employment opportunities with technology companies through a soon-to-be-launched job portal; and supporting social justice reform legislation.

[1] Internet Association, Best of the Internet Survey, June 26,2019. Available at: https://internetassociation.org/publications/best-of-the-internet-survey/.
[2] https://covid19.internetassociation.org/industry/response/.

I. Section 230 Is Critical To Content Moderation And Content Moderation Is Critical To Realizing The Value Of Online Services

In considering possible amendments to Section 230, it is vital to remember the statute's history. Congress enacted Section 230, in part, to encourage providers of online services to voluntarily adopt robust content moderation policies and practices. Congress was reacting to two lower court cases, *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991), and *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). Together, *Cubby* and *Stratton Oakmont* created a powerful disincentive for internet companies to monitor and remove objectionable content by threatening to expose companies to burdensome litigation and potential liability based on their very efforts to moderate that content.[3]

Before the enactment of Section 230, these cases presented internet companies with a difficult choice. If they voluntarily adopted content moderation policies and practices, they could end up like Prodigy—treated as a "publisher" that could be held liable for user-generated content. But if they sought to avoid this liability as CompuServe had, they would be forced to take a hands-off approach and bury their heads in the sand in an attempt to avoid acquiring

[3] In *Cubby*, a federal district court held that an interactive service provider, CompuServe, could not be held liable for allegedly false statements that a third-party had posted in one of its online forums unless CompuServe knew or had reason to know of the allegedly false statements. 776 F. Supp. at 139-141. The plaintiffs had sought to hold CompuServe liable for allegedly false and defamatory statements contained in a third party's daily newsletter that CompuServe hosted. *Id*. at 137, 140. The court noted that it would hardly be feasible "for CompuServe to examine every publication it carries for potentially defamatory statements." *Id.* at 140. In granting CompuServe's motion for summary judgment, the court analogized CompuServe to distributors of third-party content such as bookstores and newsstands. *Id*. The court explained that the requirement that such distributors "must have knowledge of the contents of a publication before liability can be imposed for distributing that publication is deeply rooted in the First Amendment." It therefore concluded that CompuServe could not be held liable unless it knew or had reason to know of the allegedly false statements. *Id*. at 140-141. Given the facts of the case—including that CompuServe exercised "little or no editorial control" over the third-party content available on its platform—the court held that the plaintiffs had failed to set forth sufficient evidence that CompuServe had the requisite knowledge, and the court thus granted CompuServe summary judgment. *Id*.

By contrast, in *Stratton Oakmont*, a New York state court held that the interactive service provider Prodigy could be held liable for allegedly defamatory statements posted on its message boards because it employed staff and used software to monitor and police content in order to attain a reputation as a "family oriented" service. 1995 WL 323710, at *2-4. The court agreed with the conclusion in *Cubby* that mere "distributors" may be liable for defamatory statements of others only if they knew or had reason to know of the defamatory statements at issue. *Id*. But the court concluded that Prodigy was instead a "publisher," liable as if it had itself made the statements, because the court viewed Prodigy as analogous to a newspaper that is "more than a passive receptacle or conduit for news, comment and advertising." *Id*. As a result, the court ruled Prodigy could be held liable for defamatory content posted on its message boards even if it lacked knowledge of that content. *Id*. The key distinction, according to the court, was that unlike CompuServe, Prodigy "held itself out as an online service that exercised editorial control over the content of messages" on its platform. *Id*.

knowledge of objectionable third-party content. This dilemma is exacerbated by the immense and rapidly increasing volume of third-party content that online platforms host and are used to disseminate, which makes detecting objectionable content exponentially more difficult. Pre-publication review cannot be scaled to match the rate at which new content is posted, and consequently, requiring it would undermine the core value of these real-time, interactive services.

Section 230 provides a thoughtful solution to the so-called "moderator's dilemma." It allows internet companies to adopt and enforce community standards without the fear that doing so would expose them to an onslaught of burdensome lawsuits. In this way, Section 230 creates critical breathing room for online providers to voluntarily undertake moderation of the unprecedented stream of content that users disseminate through their platforms. It creates a middle ground between the wild west of completely passive platforms and the closed-to-the-public realm of newspapers and other media outlets that develop and/or hand-select content for publication. That is why the statute plays such a critical role in ensuring that companies of all sizes, including IA's members, can operate the online services that the public finds so valuable.

II. Section 230 Achieves The Careful Balance It Was Designed To Create

Section 230 has been successful in achieving the goals that led to its enactment. IA member companies have adopted and enforced essential content moderation policies, just as Congress intended in enacting Section 230. In numerous areas—from child sexual abuse material (CSAM) to terrorism-related content, and from self-harm to fake reviews—IA member companies have undertaken decades-long and resource-intensive efforts to combat objectionable online content. At the same time, Section 230 has allowed the online economy to develop and prosper in the United States in ways that simply have not been replicated elsewhere around the globe. Section 230 has spurred the vibrant growth of the internet and a wide variety of diverse platforms, while also permitting internet companies to protect users, and to promote healthier online discourse, through responsible domestic and international content moderation.

A few examples can illustrate this point.

First, IA member companies take multifaceted approaches to combating CSAM on their services and in the world that are enabled by Section 230. For example, Microsoft donated PhotoDNA, image-matching software that detects CSAM, to the National Center for Missing and Exploited Children (NCMEC), so that it could be licensed for free to other entities to identify versions of previously reported CSAM. The use of existing and newly developed detection tools has significantly increased, as is evidenced by the dramatic growth in the number of CyberTipline reports in recent years. Today, IA member companies, alongside governments, civil society, and other stakeholders, continually work to stop bad actors from spreading CSAM

online. They take a variety of actions, including dedicating engineering resources to the development and improvement of tools like PhotoDNA and Google's CSAI Match, assisting in the modernization of the CyberTipline through donations of engineering resources or funds, and engaging with law enforcement agencies. Many companies also proactively detect instances of CSAM and report to NCMEC.

IA member companies have also engaged in serious efforts to eliminate content advocating or promoting terrorism. Twitter suspended 115,861 unique accounts for violations related to the promotion of terrorism during the first half of 2019.[4] Over 85 percent of those accounts were flagged by internal tools developed by Twitter itself, and many of the accounts were suspended before they ever issued even a single tweet. In the first quarter of 2020, Facebook took action on 6.3 million pieces of content supporting terrorism, with 99.3 percent of such content internally flagged before a third party reported it.[5] During the same period, YouTube removed 258,908 videos for violating its policies against violent extremism.[6] IA member companies consistently work to quickly remove any content that advocates terrorism.

IA member companies also employ a multitude of general-purpose technologies to support their content moderation efforts. IA members provide "report abuse" buttons and other mechanisms so that users can flag problematic content or contact the companies with complaints. The companies also provide specific community guidelines that provide standards for third-party content, and they devote significant staff and resources to enforcing those policies. Broad collaboration with civil society groups and other experts informs and deepens our members' commitment to safety and security. In addition, the companies have developed sophisticated software and algorithms to detect and remove harmful content. In many instances, they have shared these technologies to help others eradicate that harmful content as well. Some companies also dedicate large teams of staff that can provide quick responses to evolving problems, including responding to user complaints and removing objectionable and unlawful content. These efforts are the types of activities that Section 230 was designed to promote. It is because of, not in spite of, the law that IA members are able to take action to create safe experiences for their users.

[4] Twitter Transparency Report, Jan. - June 2019, Rules Enforcement. Available at: https://transparency.twitter.com/en/twitter-rules-enforcement.html.
[5] Facebook Transparency, Community Standards Enforcement Report. Available at: https://transparency.facebook.com/community-standards-enforcement#dangerous-organizations.
[6] Google Transparency Report, YouTube Community Guidelines Enforcement, Video Removals by Reason. Available at: https://transparencyreport.google.com/youtube-policy/removals?hl=en&total_removed_videos=period:Y2020Q1;exclude_automated:human_only&lu=total_removed_videos.

Section 230 has played a particularly important role in creating space for online platforms to refine their approaches to content moderation over time. Moderating content is not easy given the enormous volume of content online and the sometimes-nuanced distinctions that platforms must make to strike the right balance between which content to remove and which to leave up. Our member companies recognize that they do not always achieve the perfect balance, but they are constantly learning, adapting, and updating their approaches.

Section 230 allows online companies the room to experiment in this way without having to worry that they will face the heavy costs of litigation each time a mistake is made or someone is unhappy with a moderation decision. Companies can learn and make adjustments — an essential process that they engage in constantly.

The difficulty of content moderation and the importance of Section 230 is best demonstrated using an example of content that is universally hated - spam. Since the advent of the commercial internet, spammers have been intent on finding ways to flood online services with unwanted commercial messages. Their business is one of volume — if enough messages go out, even if only a small percentage are acted upon, it is profitable. The high volumes of spam messages can operate as a literal or figurative "denial of service attack." They can choke capacity of even large providers and render services of minimal value to their users by obscuring the content users want to see. It is for these reasons that spam was among the earliest targets of proactive content moderation efforts and exemplifies the challenges providers face in keeping pace with bad actors who are determined to misuse their services.

Spam detection has evolved over time from simple techniques, such as spam block lists and rate limiting on accounts to prevent any one account from sending too many messages at once, into something altogether more sophisticated. While many of the early techniques remain important tools, new algorithmic approaches that pull signals from a variety of sources are essential today. These more sophisticated tools are able to assign risk based on numerous indicators and then apply any one of a variety of interventions, including pausing account activity, requiring further account verification or passing reCaptchas to verify it is not automated activity, demoting suspect content, blocking or deleting content, and closing accounts of violators. The battle between spammers and service providers can be characterized as an arms race, as spammers quickly adapt to detection techniques and providers must continually respond. The automated systems that protect providers' services from spam may be changed on a daily, if not a more frequent, basis.

The volume of spam activity actioned by IA members is staggering. For example:

- Facebook: In the three-month period from July to September 2019, Facebook took action against 1.9 billions pieces of content for spam.[7]
- Twitter: During the first six months of 2019, Twitter received over 3 million user reports of spam and challenged over 97 million suspected spam accounts.[8]
- YouTube: In the first quarter of this year, 87.5 percent of channel removals were for violations that were related to spam, scams, and other misleading content resulting in 1.7 million channels being removed. In addition, in the same period, YouTube removed over 470 million spam comments.[9]

Section 230 is critical to these content moderation efforts. Indeed, service providers sued by spammers for removing spam have asserted Section 230 as a defense.[10] Section 230 is even more critical to efforts to address content for which there is no general global agreement that it is harmful or should be restricted. Providers develop policies across a range of issues that are extremely nuanced and uniquely tailored to their services, addressing a broad range of behaviors that are disruptive to the goal of the service they provide. There are frequently contrasting views about whether individual content moderation decisions were correct or flawed. No single solution could ever balance all of the competing visions of how content moderation ought to work. Instead, Section 230 protects a critical equilibrium that safeguards free expression and promotes user safety, while allowing providers the flexibility to respond to an ever-changing landscape of challenges in a way that best serves their users and their unique services.

III. IA's Review of Section 230 Decisions

Over a year ago, IA began reviewing court decisions involving Section 230 with a goal of developing a better understanding of how the law works in practice. Having now reviewed more than 500 decisions, IA is sharing its observations which demonstrate the need for in-depth study of this case law to inform the public policy debate over Section 230. In recent years, the national policy debate around Section 230 has focused on a few cases that garnered national media attention or specific content moderation decisions by particular providers. Employing a holistic approach will ensure that all stakeholders have a comprehensive understanding of Section 230 before advocating for changes to the careful balance that it strikes.

[7] Facebook Transparency Report, n. 5.
[8] Twitter Transparency Report, n. 4.
[9] Google Transparency Report, n. 6.
[10] *See*, *infra*, fn. 16.

IA's findings are further described in the attached paper, along with a description of our methodology and the list of decisions reviewed. IA acknowledges that the review was not comprehensive and that there are inherent limitations in attempting to draw broad characterizations from the outcome of any stage in litigation. However, we found clear patterns and observations of important note for policymakers based on judicial decisions reviewed where Section 230 immunity was implicated. IA believes that this initial effort provides a sufficient basis to support a call for a comprehensive and unbiased review of Section 230 before any action is taken to change the law. I would like to share some of our observations with you today.

A. Section 230 Benefits A Wide Range Of Entities.

IA's review of Section 230 decisions revealed that it is not only large social media companies that assert Section 230 as an affirmative defense. The importance of Section 230 is best demonstrated by the lesser-known cases that escape the headlines. Online users; internet service providers and website hosts; online newspapers; universities; libraries; search engines; employers; bloggers, website moderators and listserv owners; marketplaces; app stores; spam protection and anti-fraud tools; and domain name registrars have all asserted Section 230 immunity. These decisions show the law quietly protecting soccer parents from defamation claims, discussion boards for nurses and police from nuisance suits, and local newspapers from liability for comments posted by trolls.

It is critical to keep these smaller entities in mind when evaluating the value of Section 230. For example, in *Joyner v. Lazzareschi,*[11] Lazzareschi, a soccer parent and the operator of a local online messaging board for youth soccer called SoCalSoccerTalk, was sued by Joyner, a disgruntled soccer coach, for allegedly defamatory comments that parents made on the regional messaging board. While Lazzareschi would have fallen under the Section 230 definition of a "provider" of an "interactive computer service", the case was ultimately dismissed and the decision was upheld on appeal for Joyner's failure to meet the requirements for a defamation claim. Another example of a lesser-known entity to assert Section 230 is Allnurses.com, in the case of *East Coast Test Prep LLC v. Allnurses.com Inc.*[12] In this case, Allnurses.com, was sued by East Coast Test Prep (ECTP) because two nurses made negative remarks about ECTP's services. While this case was dismissed at the summary judgment phase for a variety of shortcomings in the plaintiff's case, Allnurses.com also successfully argued that Section 230 protected its service from liability for allegedly defamatory statements made by

[11] No. G040323, (Cal. App Jul 10, 2012).
[12] No. Civ. 15-3705 (JRT/SER), (D. Minn. Jan 26, 2018).

the nurses that used their message board to discuss topics important to the nursing field, including the relative merits of test prep providers. It is these small fora and communities, local soccer messaging boards and discussions of nursing exam courses, that would be silenced by crippling litigation without Section 230.

These examples represent just two of the seldom discussed entities that are among the wide-cross section of Section 230 beneficiaries. They are joined by local newspapers, labor unions, police associations, individuals, and others who provide spaces for users to discuss topics of interest. These entities and individuals make important contributions to the online ecosystem that exists today. During the pandemic, many of these online communities that support sharing of hyperlocal information, like the length of the line at the local COVID testing site, the health and safety measures employed by a favorite neighborhood restaurant, or resources for assistance such as food banks, play a critical role in helping us cope and recover. It is important for this Subcommittee to keep in mind the impact that changing Section 230 may have on a variety of entities and individuals within the online platform space.

B. Courts Dismiss Many Cases In Which Section 230 Is Raised As A Defense Based On Unrelated Defects In Plaintiffs' Claims.

Our review found that Section 230 is far from a "blanket immunity"[13] when it comes to the law's application in the courts. Instead our research demonstrates that only 42 percent of decisions reviewed were decided primarily based on Section 230 immunity. In over a quarter of the decisions (28 percent), the courts dismissed claims without relying on Section 230 because the plaintiff failed to state a claim upon which relief could be granted, or because of other defects in their case. Courts rejected attempts to rely on Section 230 when it was not applicable — whether because the party asserting 230 was not a covered entity, an exception applied, or the party asserting 230 was a content provider of the information at issue. Courts carefully consider the issue of the service provider's role in the creation of the problematic content, a determining factor on whether Section 230 applies.[14] When rejecting complaints based on Section 230, judges frequently explained in detail the requirements to adequately

[13] *See, e.g.*, Executive Order on Preventing Online Censorship, May 28, 2020. Available at: https://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/; Department Of Justice's Review Of Section 230 Of The Communications Decency Act Of 1996, at 4(a). Available at: https://www.justice.gov/ag/department-justice-s-review-section-230-communications-decency-act-1996?utm_medium=email&utm_source=govdelivery.

[14] *See, e.g.*, *Enigma Software Group v. Bleeping Computer*, 194 F. Supp. 3d 263 (2016); *Tanisha Systems v. Chandra*, 2015 U.S. Dist. LEXIS 177164 (N.D. Ga. 2015); *Perkins v. LinkedIn*, 53 F. Supp. 3d 1222 (2014); *Brummer v. Wey*, 2016 NY Slip Op 31021(U); *Dimetriades v. Yelp*, 228 Cal. App. 4th 294 (2014).

allege that the provider developed - in whole or in part - the content at issue, and gave plaintiffs multiple tries to amend their complaints. When plaintiffs did raise factual issues as to the service provider's role in content development, courts required discovery to allow further investigation before rendering a judgment as to whether Section 230 applied.[15]

C. Section 230 Protects Providers Who Engage in Content Moderation, But Typically Through The Application Of Section 230(c)(1)'s "Interactive Computer Service" Provision Not Section 230(c)(2)'s "Good Samaritan" Provision.

In our review, only 19 of the 516 court decisions in which Section 230 was raised as a defense were resolved on the basis of Section 230's (c)(2) "good Samaritan" clause, which provides immunity for actions taken "voluntarily" in "good faith" to restrict content that is "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." Furthermore, the majority of these cases involved provider efforts to block spam.[16] In other such decisions, courts resolved claims based on Section 230(c)(1),[17] Anti-SLAPP motions,[18] the First Amendment,[19] or for failure to state a claim or other deficiencies.[20]

Another reason (c)(2) has not been invoked more often is that, when providers are sued for removing content, many of those lawsuits are based on assertions that the provider has violated the First Amendment rights of the user whose content was removed.[21] As the First Amendment applies to only government actors, these cases have been dismissed for failure to

---

[15] *See, e.g.*, *General Steel v. Chumley*, 840 F.3d 1178 (10th Cir. 2016); *Samsel v. DeSoto County School District*, 242 F.Supp.3d 496 (N.D. Miss. 2017); *Pirozzi v. Apple*, 913 F. Supp. 2d 840 (N.D. Cal. 2012); *Cornelius v. Delca*, 709 F. Supp. 2d 1003 (D. Idaho 2010); *Best Western v. Furber*, No. CV-06-1537-PHX-DGC (D. Ariz. September 5, 2008); *Energy Automation Systems v. Xcentric Ventures*, Case No. 3:06-1079 (M.D. Tenn. May. 25, 2007); *Hy Cite v. Badbusinessbureau.com*, 418 F .Supp. 2d 1142 (D. Ariz. 2005).

[16] *See. e.g.*, *Holomaxx Technologies Corp. v. Yahoo!, Inc.*, No. 10-cv-04926 JF (PSG) (N.D. Cal. August 23, 2011), *E360INSIGHT, LLC v. Comcast Corp.*, 546 F.Supp.2d 605 (N.D. Ill. 2008); *Pallorium v. Jared*, G036124 (Cal. Ct. App. Jan. 11, 2007); *America Online, Inc. v. GreatDeals. Net*, 49 F. Supp. 2d 851 (E.D. Va. 1999).

[17] *See, e.g.*, *DeLima v. YouTube*, 2019 WL 1620756 (1st Cir. Apr. 3, 2019); *Green v. AOL*, 318 F.3d 465 (3d Cir. 2003); *King v. Facebook*, 3:19-cv-01987 (N.D.Cal. Sept 5, 2019).

[18] *See, e.g.*, *Sikhs for Justice v. Facebook*, 144 F. Supp. 3d 1088 (N.D.Cal. 2015); *Johnson v. Twitter*, No. 18CECG00078 (Cal. Superior Ct. June 6, 2018).

[19] *See, e.g.*, *Davison v. Facebook*, 370 F. Supp. 3d 621 (E.D. Va. 2019); *Estavillo v. Sony Computer Entm't Am.*, 2009 WL 3072887 (N.D. Cal. Sept. 2, 2009).

[20] *See, e.g.*, *Roberson v. YouTube*, 2018 DNH 117 (D. N.H. 2018); *Young v. Facebook*, 790 F. Supp. 2d 1110 (N.D. Cal. 2011); *Lewis v. YouTube*, No.H041127 (Cal. App. January 25, 2016)

[21] *See*, *e.g.*, *Tulsi Now, Inc. v. Google, LLC*; *Prager University v. Google LLC,* 951 F.3d 991 (9th Cir. 2020); K*amango v. Facebook, Inc.*, No. 3:11-CV-0435, 2011 WL 1899561 (N.D. NY April 19, 2011); *Davison v. Facebook, Inc.*, 370 F.Supp.3d 621 (E.D. Va. 2019); *Federal Agency of News LLC v. Facebook, Inc.*, 2020 WL 137154 (N.D. Cal. Jan. 13, 2020; *Zhang v. Baidu. com Inc.*, 932 F. Supp. 2d 561 (S.D.N.Y. 2013); *Buza v. Yahoo!, Inc.*,, No. C 11-4422 RS (N.D. Cal. 2011).

state a claim without the necessity of defendants asserting or a court analyzing Section 230. In fact, courts have found that service providers' decisions regarding whether and how to display content are protected by the First Amendment.

IV. Considerations For Policymakers

It is of the utmost importance that policymakers tread carefully when considering possible changes to Section 230 or enacting any other laws targeting content moderation. This caution is necessary because of the ever-evolving nature of harmful content and internet technology, as well as the complexity and variety of potential legal liability for online speech. This caution is also essential in light of foundational First Amendment principles.

A. Maintaining The Careful Balance Struck By Section 230.

Section 230, in its current form, supports a diverse internet ecosystem that provides users with reviews, places for discussion and lively debate, and opportunities to expand their knowledge. Without Section 230's protection, internet companies would be left with a strong disincentive to monitor and moderate content. Section 230 removes this disincentive to self-regulate, creating essential breathing space for internet companies to adopt policies and deploy technologies to identify and combat objectionable or unlawful content—or to develop other innovative solutions to address such content. Society benefits from the rules that providers voluntarily set and enforce to enhance user experiences as well as safety, goals that would be challenging - if not impossible - for the government to achieve directly due to the First Amendment. Through exceptions and carefully crafted language limiting Section 230's protections to only third-party content and activities, bad actors can still be held accountable when they participate in, or materially contribute to, illegality.[22] Over the more than two decades since Section 230's enactment, the internet continues to thrive due to the carefully crafted language balancing the fostering of online innovation with ensuring there are proper ways to hold content providers accountable for their actions.

B. Ensuring That Any New Requirements Recognize The Flexibility Required For Effective Content Moderation.

Some proposals to change Section 230 have the potential to impact how service providers conduct content moderation by limiting the protections in the statute to just certain types of content, or setting new rules for how companies engage in content moderation activities. Policymakers considering making changes to Section 230 must recognize the wide cross-section of online services that rely on the law and keep in mind the need for flexible and

[22] *Fair Housing Council of San Fernando Valley v. Roommate.com*, 521 F.3d 1157, 1168 (9th Cir. 2008) (*en banc*). In addition, Section 230(e) outlines the criminal law, intellectual property, state law, communications privacy law, and sex trafficking law exemptions from 230 immunity.

non-prescriptive language. There are important reasons why the broad group of entities and individuals who qualify as providers of interactive computer services should be able to retain discretion and flexibility to set and enforce their rules. For example, content moderation teams should be encouraged to be nimble enough to respond to unanticipated events quickly. The urgent nature of the response to the video of the Christchurch attack is a good example of how world events can impact content moderation efforts. The circumstances of the Christchurch attack are precisely why providers need to be able to make adjustments to the techniques they use to battle policy violations to adapt alongside the ever-evolving nature of threats. Imposing overly prescriptive and burdensome requirements through legislation or regulations will negatively impact the internet ecosystem. Without flexibility, service providers are unable to effectively moderate content on their platforms, which could dramatically reduce the quality of their services. Furthermore, online platforms are not uniform in their breadth, construction, business models, or approach to content hosting. Changes to Section 230 intended to address concerns with a particular platform or type of platform, will impact all platforms. Given the discrete but important differences among internet platforms, changes to Section 230 must carefully consider the broad and varied impacts of legislative language on different platform models.

C. Aligning With Established First Amendment Principles That Apply To Content Moderation.

Any amendments to Section 230, and any other laws pertaining to content moderation, should take careful account of three First Amendment guardrails.

First, platforms are not state actors and consequently need not refrain from moderating speech protected by the First Amendment. The First Amendment only limits the actions of state actors—that is, governmental entities—not private companies merely because those companies provide forums for speech. Courts have consistently held that internet platforms are not state actors bound to follow the strictures of the First Amendment.[23] Plaintiffs cannot bring suit against platforms alleging that the platforms somehow violated the plaintiffs' right to express particular speech under the First Amendment. Some have suggested that social media sites should be treated as public forums subject to First Amendment restrictions. However, most users would not want the First Amendment to dictate internet platforms' content moderation practices as though they were state actors. If that were to happen, platforms would be prevented from blocking or screening a wide-range of problematic content that courts have held to be constitutionally protected including pornography, hate speech, and depictions of violence.

[23] *See*, *e.g.*, F*reedom Watch, Inc. v. Google Inc.*, 2020 WL 3096365, at *1 (D.C. Cir. May 27, 2020) (per curiam); *Prager Univ. v. Google LLC*, 951 F.3d 991, 996-999 (9th Cir. 2020).

Second, the First Amendment protects the rights of the platforms themselves. When platforms determine what kind of platform to be and what kinds of content to host or prohibit, those are forms of free expression protected by the First Amendment. It is bedrock First Amendment doctrine that such editorial decision-making is constitutionally protected. In *Miami Herald Publishing Co. v. Tornillo*,[24] for instance, the Supreme Court held that a statute requiring newspapers to provide political candidates with a right of reply to critical editorials violated the newspaper's First Amendment right to exercise "editorial control and judgment" in deciding the "content of the paper."[25] Several courts have applied this reasoning in the online context, holding that platforms possess the First Amendment right to decide what content to carry.[26] Recognizing this principle has never been more important. It is critical to allowing online communities and services to develop around common interests, shared beliefs, and specific purposes. It is also critical to allowing online services to cater to different audiences, including the ability to design rules to make their services age-appropriate or purpose-appropriate.

Third, the First Amendment sets a constitutional floor that ensures that online platforms that carry vast quantities of third-party content cannot be held liable for harms arising from that content based on a standard of strict liability or mere negligence. Applying such non-protective standards of liability to entities that distribute large volumes of third-party material would violate bedrock First Amendment principles. The Supreme Court examined this issue over six decades ago, in *Smith v. California* .[27] There, a city ordinance prohibited bookstores from selling obscene or indecent books regardless of whether the store owners knew the books were obscene or indecent.[28] The ordinance violated the First Amendment, the Court explained, because it would cause a bookseller to "restrict the books he sells to those he has inspected" and thus "impose a severe limitation on the public's access to constitutionally protected matter."[29] This principle—that the First Amendment gives special protection to those who act as clearinghouses for large quantities of third-party content—applies with especially great force to internet platforms, given the exponentially greater volumes of content that they host and the important role they play in societal discourse. Were these platforms to face liability for distributing unlawful third-party material absent circumstances in which they both knew of that particular content and yet failed to remove it, internet users' access to vital constitutionally protected speech would be severely stifled.

[24] 418 U.S. 241 (1974).
[25] *Id*. at 258.
[26] *See*, *e.g.*, *Jian Zhang v. Baidu.com Inc.*, 10 F. Supp. 3d 433, 436-443 (S.D.N.Y. 2014); *Langdon v. Google, Inc.*, 474 F. Supp. 2d 622, 629-630 (D. Del. 2007).
[27] 361 U.S. 147 (1959).
[28] *Id*. at 148-149.
[29] *Id*. at 153.

This trio of First Amendment principles provides important constitutional guardrails that protect free expression on the internet. Along with Section 230, they have contributed to making the internet a vibrant medium that benefits so many. Policymakers addressing content moderation must therefore carefully consider the interaction between these principles and new policies before enacting new laws that could threaten to undermine the constitutional foundation of our dynamic internet.

V. The PACT Act

Given the many crucial considerations implicated by any proposal to amend Section 230, IA appreciates the thoughtful approach taken by Senators Schatz and Thune in the ‘‘Platform Accountability and Consumer Transparency Act’’ or the ‘‘PACT Act.’’ IA and its member companies appreciate the focus in the bill on the twin goals of promoting transparency and accountability in content moderation. Over the last several years, IA member companies have been working continuously to enhance transparency with their users and the public about their community rules; how they are enforced; and how often they are enforced. These efforts include expanding transparency reporting to cover a wider range of topics including content removals for terms of service violations, making the rules of the service easier to understand and more detailed, providing additional user education and guidance through examples of potential rule violations, and explaining in more detail how rules are enforced and the potential consequences for violations. These efforts are just one part of how IA member companies approach content moderation and supplement measures such as easy reporting of violating content, user notices and appeals, and proactive efforts to find violating content. The PACT Act’s focus on these aspects of content moderation in many ways align with IA member company efforts, and for that reason, IA hopes to work with the sponsors to ensure that the bill is able to achieve its goals without inhibiting flexibility and innovation in content moderation.

IA would like to highlight two areas of concern related to the bill’s broad scope and highly detailed requirements. With regard to the bill’s scope, the requirements for transparency and accountability in Section 5, as drafted, would apply to all “interactive computer services” (ICSs), which is essentially the same group of entities that benefit from the protections of Section 230. As discussed above, Section 230 applies to a wide-range of interactive services and platform models including those offered by individuals, informal clubs or groups, and member associations. In addition, the types of services that fit within the term “interactive computer service” are likewise broad, covering not only social media services, but also private messaging, search, message boards and listservs, dating services, job search platforms, review sites, and more. IA is concerned that the requirements of Section 5 would prove too large a burden for those ICSs as hobbyists, volunteers, and as adjuncts to other activities. Such requirements may force these individuals and entities to shut down their projects and may discourage similarly situated individuals and groups from engaging in important expressive activity. There are also services for which transparency requirements may not make sense given the type of service or the purpose for which it was created. For example, under Section 5,

review platforms would have to disclose to fraudsters (e.g. rival businesses or competitors of the business being reviewed) that their fake reviews had been detected and give fraudsters an opportunity to appeal the takedown of their fake review. While transparency is often a benefit, the burdens associated with these particular requirements should be carefully weighed against the benefits they would likely achieve. For this reason, IA hopes to work with the sponsors to consider potential changes to the scope of the bill.

The other potential issue IA would like to share regarding the bill relates to the negative ramifications the highly detailed requirements in Section 5 could have. First, the detailed nature of the requirements would be extremely burdensome for all ICSs, and it would be a struggle for all but the most highly resourced providers to comply. For example, in order to comply with transparency reporting requirements, providers would need to rebuild the systems they use to process and track user reports, as well as any systems that operate independently to moderate content, to ensure that all of the required types of information are collected for future reports. Absent a long window to ramp up, providers may need to manually review each individual report to collect information for backwards-looking reports. The difficulty of complying could adversely impact content moderation as providers may choose to narrow their content policies to limit the scope of issues that would have to be addressed by the requirements of Section 5. Therefore, these requirements could unintentionally result in *less* moderation, rather than more.

As with the scope of the bill, the Section 5 requirements would likely limit the diversity and richness of the different types of individuals and entities that are part of the online ecosystem. This in turn would limit consumer choice and access to information. Small providers in particular would feel the impact of these requirements. In addition, the detailed nature of the requirements would significantly diminish the essential flexibility providers have today to constantly adjust their approaches to content moderation to keep pace with bad actors, respond to emergencies, and focus their efforts on the activities that pose the highest risks to users of their services and the public.

IA appreciates the opportunity to discuss the value of Section 230 to the modern internet and looks forward to continuing these conversations around our concerns and other feedback pertaining to this bill with the members of the Subcommittee.

APPENDIX: Internet Association, *A Review Of Section 230's Meaning & Application Based On More Than 500 Cases* (July 27, 2020).