Documents for the Record – 04.11.24 C&T Hearing

1. A statement for the record from the Internet Society.
2. A letter to committee leadership from Taxpayers Protection Alliance.
3. A letter to committee leadership from Engine.
4. A statement for the record from the Alliance for Safe Online Pharmacies.
5. A New York Times article titled, “Teen Girls Confront an Epidemic of Deepfake Nudes in Schools.”

STATEMENT FOR THE RECORD

OF THE

INTERNET SOCIETY

COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

UNITED STATES HOUSE OF REPRESENTATIVES

HEARING: "WHERE ARE WE NOW: SECTION 230
OF THE COMMUNICATIONS DECENCY ACT OF 1996"

APRIL 11, 2024

Chairs Rodgers and Latta and Ranking Members Pallone and Matsui, thank you for holding this hearing regarding Section 230 of the Communications Act of 1934, as amended by the Telecommunications Act of 1996. The Internet Society is pleased to submit this statement for the hearing record.

Founded in 1992, the Internet Society is a US non-profit organization headquartered in Reston, Virginia, and Geneva, Switzerland, with a core mission of promoting and defending the Internet. The Internet Society's staff comprises technical experts in internetworking, cybersecurity, and network operations, among other fields, as well as policy experts in a broad range of Internet-related areas.

A key characteristic of the Internet—one that sets it apart from every other communication medium—is that it was meant to be open for everyone. Individuals can speak, debate, create, invent, and engage with others, whether they are across town or around the world. The broad protections that Section 230 affords are essential for—in the words of that statute—this "interactivity" on the Internet. Simply stated, without the basic protections that Section 230 provides, we would not have the robust engagement of hundreds of millions of Americans in the online conversation, nor would we have the astounding innovation in online services that we have witnessed over the past 25 years.

It is certainly true that as more of our society's discourse has moved online, so have several serious societal problems. We appreciate that Congress is looking to address some of those problems. Americans are, quite reasonably, concerned that speech and behavior that would not be tolerated in other settings are seemingly not only protected, but even exploited for profit, in some online platforms. At the same time, the power of those very platforms appears only to grow, such that they have outsized influence and power in the social and political life of the

nation and other nations around the world. Yet, it is important not to lose sight of the value of the Internet. For every appalling example of childhood sexual abuse material, there is an example of a young person who was in crisis and found online a community of others like themselves. Examples of nasty online speech abound, but so do examples of people reaching out and giving one another support in times of need. Some consumers of content on platforms appear to see only polarizing influences, but plenty of others seem to use the same platforms for education and thereby to better themselves. The Internet can be a conduit for social harm, but it has also proven to be an enormous resource for social good. Any changes to the rules about its operation must be undertaken with enormous care.

Our core message to this Subcommittee is that—because of its critical role in ensuring the very ability of individuals to speak online—Section 230 is not the appropriate vehicle through which to try to address social problems. Amendments to Section 230 risk the viability of what makes the Internet unique—the ability of individuals to participate in the global marketplace of ideas.

To appreciate these risks, we must all remember why Congress took the bold steps to create Section 230 in the first place. It was a very early stage of development of the public Internet—and the legal landscape that applied to it—that Congress confronted when it enacted what became Section 230. But in its wisdom, Congress created the broad scope of protections that Section 230 affords far beyond the major online platforms that have since emerged. As a result, there are serious risks that would flow from removing those protections. We address each of these points below.

A. THE ORIGINS AND GOALS OF SECTION 230

The Internet was developed in the 1970s (by some of the founders of the Internet Society, among others) within the US academic community through a federal government project.[1] Even at this early stage, the potential for interactivity—individual participation—unique to the Internet was plain. In the 1970s and 1980s, it was used primarily for collaboration between academic, government, and commercial researchers, with non-research commercial traffic effectively prohibited. The broad ban on commercial activity—including commercial services offered to individuals—lasted until the Internet was transitioned to the private sector, in April 1995, about nine months before Section 230 was enacted.[2]

The Internet's design is somewhat peculiar in that it is not a single system, but rather a system built up from other systems. This nature is immediately apparent from its name—the Inter-net. The designers recognized that the best way to deploy a very large, distributed network was to take advantage of various other, existing networks, and link them together with some basic common technology. This fundamental design of the Internet is what has allowed it to grow so large. As new needs, areas of operation, or inventions come along, new networks can

[1] Vint Cerf, *A Brief History of the Internet and Related Networks*, Internet Society, https://www.internetsociety.org/internet/history-internet/brief-history-internet-related-networks/.
[2] *See A Brief History of NSF and the Internet*, National Science Foundation (Aug. 13, 2003), https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050.

join the Internet without adjusting the rest of the system. This feature of the design is especially relevant for any consideration of changes to Section 230, because it creates many different actors whose actions might be implicated in any liability question.

Over the 1970s and 1980s, privately-operated networks were also created, ranging from commercial-focused communications networks to "bulletin board" services for individuals or small groups to communicate. As early as 1992, a newspaper reported that "computers [are] growing as [a] forum for ideas"—the newspaper reported on a political debate through a bulletin board involving individuals in Wethersfield, CT, St. Louis, MO, and Glendale, AZ.[3] One of the earliest successful private networks—CompuServe—was founded in 1969 as a "dial up" network aimed at businesses, before later offering its services to individuals, who were then able to engage, share content, and collaborate with people far beyond their local communities. As restrictions on commercial traffic on the Internet eased, these other networks also had the opportunity to join the Internet, bringing even more people into one global online community even as they continued to receive service from their preferred service provider.

As with all forms of communication since the emergence of the common law, there arose the question of how liability for harmful or illegal content would be assigned in the online context. With "first-party" speech—where the speaker and the platform for speech are the same entity—liability was always clear: the first-party speaker would be liable. What was unclear was responsibility for "third-party" speech—speech by speakers that was carried or conveyed by others. Throughout the history of this country, the rules for responsibility for third-party speech under the common law have appropriately varied by the medium of the speech:

- **Broadsheets, pamphlets, and speech on the village green:** Generally, there was no third-party speech involved, and thus only first-party liability applied.
- **Newspapers:** Most speech is first-party speech, but the newspapers can be liable for third-party speech (such as letters to the editor).
- **Telephones:** Under the common carriage regime, telephone companies were not liable for speech made over their networks.
- **Radio and broadcast television:** Similar to newspapers, with potential liability for the broadcaster if they carry third-party speech.
- **Cable television:** Through private negotiations between the cable channels and cable systems, liability was allocated to the cable channels.

But the Internet is fundamentally different than any of those media, with literally hundreds of millions of people and entities involved in the liability questions. In the 1990s, two seminal cases began to answer the question of whether online service providers would be liable for content posted by individual users. *Cubby, Inc.* held that an online service provider would not be held liable for speech made by a participant in an online forum, but *only* because the provider

[3] Hartford Courant, Computers Growing as Forum for Ideas, Aug. 17, 1992 (available at https://www.courant.com/1992/08/17/computers-growing-as-forum-for-ideas/). The article identified one political observer who saw "the beginning of a vast change in how people learn about and discuss politics," quoting him as saying: "There are 65 million computer users in the United States, and they're just starting to use their modems."

had not moderated any content. *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991). Then *Stratton Oakmont, Inc.* held an online service provider liable for participants' speech because the provider engaged in some content monitoring and regulation. See *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). These cases created significant uncertainty and potentially crippling liability for the developing industry of online service providers, including companies that facilitated access to the Internet and third-party speech.

It is against this backdrop that Congress considered and enacted the "Internet Freedom and Family Empowerment Act," which became 47 U.S.C. Section 230.[4] One of Congress's explicit goals for Section 230 was "to promote the continued development of the Internet and other interactive computer services and other interactive media." 47 U.S.C. 230(b)(1). Congress recognized that interactive computer services in general, and the Internet in particular—even at its early stage when Section 230 was enacted—offered what was at the time a profoundly unique platform for interactive communication. Congress observed in the statute that the "Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity." *Id.* 230(a)(3). In Congress's judgment in 1995, these interactive communications, which foster public discourse, should be encouraged. The Internet, unlike prior "published" forms of mass communication, transforms the individual from a passive recipient of mainly corporate-created products into an active participant in shaping communication and content. Congress recognized that this individual-driven "interactivity" was an essential attribute of the emerging Internet that warranted protection.

The results of the Congressional foresight to enable citizen speech and innovation are undeniable. A vast amount of communication (artistic, political, intellectual, pedestrian, and otherwise) now flows through the Internet—whether through blogs, message boards, social media both large and small, videos or music uploaded to the Internet, or other means. Already by

[4] The "Internet Freedom and Family Empowerment Act" passed almost unanimously by the U.S. House of Representatives in part *as an alternative to*—not a part of—the "Communications Decency Act" (CDA), which had been proposed and passed by the United States Senate. A joint Senate-House conference committee decided to include *both* the CDA and House-passed Internet Freedom and Family Empowerment Act in the Telecommunications Act of 1996. When the Telecom Act was assembled into a single bill after the conference committee, the Internet Freedom and Family Empowerment Act was placed into a section of the Telecom Act immediately following the nine sections that comprised the CDA. Section 230 was never a part of the Senate-passed CDA, and the incorrect lumping of Section 230 into the CDA continues today to cause confusion about the intent of Section 230 (*i.e.,* the Internet Freedom and Family Empowerment Act). CDA's rules on "indecent" and "patently offensive" content were quickly challenged and subsequently struck down on First Amendment grounds by the United State Supreme Court in Reno v. ACLU, 521 U.S. 844 (1997), but Section 230 had not been challenged and was not at issue in the Reno decision. *See* Ashley Johnson & Daniel Castro, *Overview of Section 230: What It Is, Why It Was Created, and What It Has Achieved*, ITIF (Feb. 22, 2021), https://itif.org/publications/ 2021/02/22/overview-section-230-what-it-why-it-was-created-and-what-it-has-achieved.

1997, the U.S. Supreme Court noted in its *Reno* decision the "dramatic expansion of this new marketplace of ideas," and the Court held that speech on the Internet warrants the highest level of Constitutional protection under the First Amendment.[5] In that case, the lower court had observed the beneficial "democratizing" effects of Internet interactivity and noted, "that the Internet has achieved, and continues to achieve, the most participatory marketplace of mass speech that this country—and indeed the world—has yet seen."[6]

B. THE BROAD SCOPE OF SECTION 230 PROTECTIONS

As this Subcommittee examines the purposes of Section 230 and highlights the growth of information technology companies since the law's inception, it is vital to understand that Section 230 protects providers and individuals far, far beyond the major online content platforms. Section 230 is applicable—and needed—at almost every level and in every corner of the Internet ecosystem.

Foremost—and often overlooked in discussions of Section 230—is that it directly and critically protects hundreds of millions of Internet users in America. In addition to companies and organizations that offer Internet and online services, Section 230 also specifically protects "users" of those services. Thus, every time that an American re-tweets a humorous or outrageous tweet, they are protected by Section 230 in the event that the original tweet is found to be defamatory or otherwise harmful. Similarly, every time an American on social media forwards an interesting newspaper article or a hard-hitting online restaurant review, they are protected by Section 230 from liability for the underlying content.

Beyond this type of common user engagement that is protected by Section 230, individual Americans—as well as many community groups, political organizations, and local governmental agencies—are protected by Section 230 when they host discussion forums online that allow other people to discuss a topic. Here are just a few examples of the thousands—if not hundreds of thousands—online discussion fora:

- The "r/Spokane" forum on Reddit has 57,000 members and bills itself as the "place to engage on all things in the greater Spokane [Washington] area and the Inland Northwest," at https://www.reddit.com/r/Spokane/;
- the "Spokane Reservation General Public Forum" is a discussion forum with more than 1,500 participants "for Tribal Members, Affiliated family and friends" intended to "gather and exchange important information that affects the Spokane Indian Reservation and the Community as accurate as possible for discussion," at https://www.facebook.com/groups/2661505284175799/;
- a blog run by the Municipal Manager for Lawrence Township, NJ, seeks to "engage the Lawrence community in a more personal and substantive way," at https://lawrencetownshipnjmanagerkpn.blogspot.com/;

[5] *Reno v. American Civil Liberties Union*, 521 U.S. 844, 885 (1997).
[6] *Am. Civil Liberties Union v. Reno*, 929 F. Supp. 824, 881 (E.D. Pa. 1996).

- the Ohio Election Forum hosts, for 3,200 members, a public Facebook Group that provides "a neutral Forum where your Conservative candidates and officials can interact," at https://m.facebook.com/groups/290345189599995/;
- "Eleven Warriors" – which states that it is "the largest independent sports site on the internet and is a one-stop shop for Ohio State news, analysis and community," hosts extensive open discussion forums about Ohio State football, at https://www.elevenwarriors.com/forum/ohio-state-football, and
- "KingsFans.com" hosts numerous very active discussion groups covering basketball and non-basketball topics for fans of the Sacramento, CA, Kings team, at https://community.kingsfans.com/.

As may be obvious, there is a huge diversity of online discussion groups in every state across the country, most of which are hosted by individuals, small organizations, government agencies, and others. And of course there is a vast array of national discussion fora, ranging from https://liberalforum.net to https://conservativepoliticalforum.com, and from https://www.reddit.com/r/Cooking/ to https://www.gardenstew.com/, and from https://racing-forums.com/forums/nascar-chat.8/ to https://www.reddit.com/r/rugbyunion/. Every person and organization hosting or moderating those discussion groups is directly protected by Section 230 for liability for content posted in their fora by other people.

Beyond the non-commercial sites identified above, many commercial entities also host comments from customers, users of their products, and people interested in their work. Some small online retailers allow customers to post reviews of their products, some newspapers (such as the Seattle Times) allow readers to post comments, and there are numerous software and service providers aimed at enabling small businesses to build interactive online communities of their customers. Any of these small businesses that allow customers, users, or the public to post comments are directly protected by Section 230.

In addition to the participation of individuals and small organizations on the Internet, of great concern to our organization is that Section 230 also protects many different types of service and infrastructure providers in the Internet ecosystem. Those providers include (but are not limited to):

- Internet Service Providers ("ISPs"), who make it possible for individuals to access the Internet. Whether through cable, digital subscriber lines, fiber, wireless, or satellite connections, ISPs enable Internet access. Section 230 ensures that ISPs are not responsible for regulation and monitoring of third-party content transmitted over these services. According to BroadbandNow, there are in the United States "more than 2,906 Internet service providers, with most covering very small areas." This includes, for example, about 50 ISPs in Washington State (with 32 in Spokane alone), about 20 ISPs in New Jersey (with 18 in New Brunswick), more than 40 in Ohio (with 20 in Bowling Green), and about 50 ISPs in California (with 32 in Sacramento).[7]

[7] *See* https://broadbandnow.com/Washington, https://broadbandnow.com/New-Jersey, https://broadbandnow.com/Ohio, https://broadbandnow.com/California.

- Content Delivery Networks (CDNs), which are specialized network providers, also depend on Section 230 immunity. CDNs are geographically distributed networks of proxy servers and data centers, and they are crucial to delivering large amounts of data (such as delivering high-definition streaming video) quickly to many viewers simultaneously.
- Web hosting companies, many of which, around the country, specialize in helping local small businesses get online. Section 230 is critical to their existence.

Each of these types of infrastructure providers—and others—depends on Section 230 to enable them to efficiently convey traffic to the final destination without risk of liability or obligation to screen content passing through their networks. That includes operators of systems—such as ISPs or voice-over-IP providers—that have no involvement at all with the content that passes through their systems. Like the individuals discussed earlier, their ability to fully participate in the online ecosystem is heavily dependent on the continued protections under Section 230.

C. SERIOUS RISKS FROM REDUCING SECTION 230 PROTECTIONS

A complete repeal of Section 230 would be immediately catastrophic to the Internet, the hundreds of millions of Americans who use and engage online over the Internet, and the tens- or hundreds-of-thousands of businesses in this country that directly offer Internet-based services. The thousands of very small Internet Service Providers—which provide Internet access to many thousands of small, rural, and underserved communities across this country—would immediately be at grave risk of being sued for harmful content transmitted over their networks. And even if they might ultimately prevail in such lawsuits, the costs of litigating can be crushing and could easily put them out of business. Many more thousands of other businesses would similarly face grave risk for providing online services. And over time, as the understanding of the risks became clearer, many businesses would simply choose to shut down. Only the very largest players in the various markets—ISPs, web hosting providers, online platforms—could safely be predicted to survive.

But an even graver risk is that Congress will consider and enact a more limited "reform" of Section 230 that—as a practical matter for individuals and small businesses—would have the same basic effect of a total repeal. Amendments that carve out new exceptions or add new limitations to Section 230 could easily create too much risk of liability for individuals and small businesses. The vast majority of the individuals and entities protected by Section 230 do not even remotely have access to the resources—or lawyers—that are available to the major online platforms. Many if not most businesses in America would be severely threatened by facing even a single serious lawsuit (especially one that cannot be quickly dismissed as Section 230 permits), and an increase in litigation risk for online speech would drive some companies out of businesses, and would certainly discourage other potential start-ups from entering the field at all.

These risks of liability would profoundly damage the ability of users to speak and receive information online. Providers facing the risk of crippling liability would rationally decide not to carry user or other third-party speech at all, or to carry only a very limited amount that it could be confident would not subject it to liability (e.g., because it was entirely non-controversial or

came from an "authoritative" source). In other words, repealing or substantially limiting Section 230 would reduce the opportunity for users of all stripes to engage in speech online.

The reason for this danger goes back to the very nature of the Internet itself. Because it is a distributed network of other networks, there is no central point of control, and a huge abundance of parties involved in its operation. Many of the proposals that appear to address the societal problems the United States faces are, really, efforts to address the behaviors of small handfuls of organizations involved in the operation of the Internet, or even merely services that depend on the Internet. But any changes to Section 230 risk involving all of those other organizations that make the Internet such a resource for all humanity. That is why it is so important to recognize why Section 230 covers so much: it must, because the diversity of people involved in making the Internet is so large.

Because Section 230 protects the entire Internet ecosystem—and the very ability of individuals to participate online—it is a very poor vehicle through which to seek to address problems caused by a small subset of bad actors, actors who may or may not be covered by Section 230. This is not to say that Congress is powerless to address important social problems. Approaches that give rights to all Americans—such as baseline privacy legislation[8]—would be an important start to address some of the current lack of protections in the online sphere. More direct regulation of certain categories of online services could also be appropriate in some cases.[9] And, although we have not seen any examples proposed to date, we do not reject the logical possibility that a focused amendment to Section 230 might achieve socially desirable goals without gravely undercutting the Internet. The Internet Society certainly stands willing to consult and provide feedback on any proposals to address social problems online.

CONCLUSION

Online content can raise difficult concerns—concerns appropriate for Congress to consider addressing. But any action by Congress should not come at the cost of the enormous positive benefits that have flowed, and continue to flow, from the fact that hundreds of millions of Americans are able to go online and express their opinions, share their creative works, pursue innovative and sometimes lucrative new ideas, and generally engage in the global online conversation.

We appreciate the opportunity to submit this statement to this Subcommittee, and we would welcome an opportunity to testify on these topics at a later hearing, or meet with your staff about Section 230.

---

[8] We commend this Committee's recent actions on privacy.

[9] It is also true that *any* new U.S. law responding to categories of speech online—whether altering Section 230 or not—will face significant constitutional hurdles. The vast majority of speech online—even some harmful or unwanted speech—is lawful under the First Amendment. Private companies that offer Internet-based services themselves have First Amendment rights to carry—or not carry—any lawful speech, and contrary to some misunderstanding, the free speech and moderation rights of private platforms flow from the First Amendment, not Section 230.

TAXPAYERS PROTECTION ALLIANCE

April 10, 2024

The Honorable Bob Latta
Chair
Energy and Commerce Committee
Communication and Technology Subcommittee
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Doris Matsui
Ranking Member
Energy and Commerce Committee
Communication and Technology Subcommittee
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515

Re: April 11, 2024, Hearing Entitled: "Where Are We Now: Section 230 Of The Communications Decency Act Of 1996"

Dear Chair Latta, Ranking Member Matsui, and Members of the House Committee on Energy and Commerce's Communications and Technology Subcommittee,

The Taxpayers Protection Alliance (TPA) is a nonprofit, nonpartisan taxpayer, and consumer watchdog organization. Ahead of this week's hearing in the House Committee on Energy and Commerce's Communications and Technology Subcommittee on 47 U.S. Code § 230 (Section 230), TPA encourages the committee to consider the delicate balance struck by the statute and reject the many myths and misplaced sensationalism that have come to surround it.

Section 230 says, exclusively for the purposes of civil cases (tort law), people are responsible for what they post online, not necessarily where they post it or who shares it.[1] The law places civil liability for content squarely at the feet of the producer of that content, not the provider of the tool used. In doing so, Section 230 is responsible for both one of the greatest expansions of free speech and expression ever while empowering private actors to protect vulnerable populations from content that may be harmful to them, even if that content is otherwise legal.

Alteration or elimination of Section 230 in pursuit of noble goals of further protecting vulnerable populations or expanding user speech protections make perfect the enemy of the good. Common suggestions to alter the statute each present unacceptable tradeoffs that run counter to taxpayer and consumer interests as well as many express interests of members of Congress across the political spectrum.

Below are several clarifications to common critiques and policy suggestions regarding Section 230 that TPA hopes will guide members of the subcommittee in their questions and thinking about this critical statute.

A world without Section 230 runs counter to other congressional interests

In considering reforms to Section 230, the state of the law prior to its enactment must be considered. Former Representative Chris Cox (R-Ca.), one of the authors of Section 230, offers this summary of the relevant precedent at the time:

> "New York courts took the lead in deciding that an internet platform would bear no liability for illegal content created by its users. This protection from liability, however, did not extend to a platform that moderated user-created content. Instead, only if a platform made no effort to enforce rules of online behavior would it be excused from liability for its users 'illegal content. This created a perverse incentive. To avoid open-ended liability, internet platforms would need to adopt what the New York Supreme Court

[1] 47 U.S. Code § 230 has no bearing on criminal law. See § 230(e)

> called the 'anything goes' model for user-created content. Adopting and enforcing rules of civil behavior on the platform would automatically expose the platform to unlimited downside risk."[2]

If Section 230 were to disappear overnight, the existing precedent would suggest that the most effective ways for an online service provider to shield itself from civil liability would be to allow for any and all content to be posted without moderation or disallow third party user posts entirely. In the former case, harmful content of all stripes would proliferate online causing untold damage. Free expression and speech would also suffer, as benign user-generated content would be drowned out and user audiences would be driven away in a phenomenon akin to a Heckler's Veto. In the latter case, many online services would be relegated to nothing more than digital versions of traditional print and broadcast media, with the barriers to speech and commerce the internet has smashed rebuilt to a degree that would seem utterly suffocating compared to the status quo.

The third option for a service seeking to mitigate risk of civil liability, but still allow user-generated content, would be to engage in substantially more aggressive content moderation. To some critics of Section 230, this is precisely the outcome they seek to avoid, given rampant accusations of bias and censorship against the leading technology firms. To the critics of Section 230 concerned with the volume of harmful content online, this may sound like an ideal outcome. The reality is that this path is only available to those firms with the resources to implement extremely complex and expensive systems of content filtering and moderation as well as fend off litigation when it inevitably arises. In short, the effect of repealing Section 230 would be to dig a moat around the largest online service providers of today and make it effectively impossible for new competitors in the user-generated content space to reach scale.

Section 230's constitutional lynchpins

Section 230 is under fire from critics across the political spectrum largely due to disapproval of various content moderation decisions by online service providers. There is anger at both action and inaction by providers. Section 230 names the kind of content Congress wishes to curb online: "[O]bscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable[.]"[3] Some feel companies have not done enough to combat this type of content while others feel service providers have acted against content beyond these categories and therefore beyond what Congress intends.

Yet, efforts to further hone Section 230 to bring the content moderation decisions of service providers closer to reflecting any given view of what constitutes "filthy" or "excessively violent," for example, would put the entire law in constitutional jeopardy, thus endangering the immunity conferred to firms making uncontroversial moderation decisions as well. The same problem exists with trying to exclude from immunity decisions over content not explicitly mentioned in the statute, such as political speech. The First Amendment significantly constrains Congress's ability to further designate or delineate kinds of moderation decisions it wishes to immunize, or picking winners and losers among protected speech.
The statute as currently written avoids the glaring constitutional issue of favoring or disfavoring otherwise protected speech by explicitly leaving the task of defining the excessive and objectionable to "the provider or user"[4] of interactive computer services, not Congress. Any blurring of this current bright line through additional caveats and clarifications as to what Congress considers "objectionable" in the realm of protected speech faces enormous constitutional hurdles. Congress simply cannot direct the moderation decisions of firms, thereby outsourcing censorship. It can only protect the ability of firms to exercise their own First Amendment rights of speech and association as well as property rights, as Section 230 does now.

[2] Cox, Christopher, "Section 230: A Retrospective," The Center for Growth and Opportunity at Utah State University, November 2022. https://www.thecgo.org/research/section-230-a-retrospective/
[3] 47 U.S. Code § 230(c)(2)(A)
[4] Ibid.

Congress should not condition immunity on political neutrality

Some have suggested anchoring the kind of tort immunity provided by Section 230 to a standard of political or viewpoint neutrality. There are significant legal and practical reasons as to why Congress should not do this.

Mandating political or viewpoint neutrality is often categorized as a form of common carriage regulation. Christopher S. Yoo, a law professor at the University of Pennsylvania and founder of the Center for Technology, Innovation and Competition at the university argues such a designation does not circumnavigate the inherent First Amendment issues of mandating platforms to host certain speech against their desires:

> "Courts and legislatures have suggested that classifying social media as common carriers would make restrictions on their right to exclude users more constitutionally permissible under the First Amendment. A review of the relevant statutory definitions reveals that the statutes provide no support for classifying social media as common carriers. Moreover, the fact *that a legislature may apply a label to a particular actor plays no significant role in the constitutional analysis*. [emphasis added] A further review of the elements of the common law definition of common carrier reveals that four of the purported criteria (whether the industry is affected with a public interest, whether the social media companies possess monopoly power, whether they are involved in the transportation and communication industries, and whether social media companies received compensating benefits) do not apply to social media and *do not affect the application of the First Amendment.* [emphasis added] The only legitimate common law basis (whether an actor holds itself out as serving all members of the public without engaging in individualized bargaining) would again seem inapplicable to social media and have *little bearing on the First Amendment.* [emphasis added]"[5]

In addition to the First Amendment hurdles, as a practical matter viewpoint neutrality on private, widely available online spaces is not a desirable outcome with respect to Congress's goal outlined in the text of Section 230 (the private filtering of "objectionable" material). There are also ongoing and growing concerns about foreign influence, espionage, and other hostile operations on online platforms. While Section 230 provides no panacea on these issues, conditioning immunity on viewpoint neutrality would only exacerbate these issues by creating a strong disincentive for online service providers to take swift action against overt misuses or questionable uses of their services.

It is critical for lawmakers to remember that the scope of protected political speech and viewpoints extends well beyond what can be found represented in the halls of the United States Capitol. Speech that is widely viewed as acceptable, even if not widely agreed with, generally does not need protection. Views commonly regarded as bigoted, violent, or otherwise harmful enjoy equal protections to run-of-the-mill political speech under the Constitution. Congress cannot elevate the latter without inherently amplifying the former. The Constitution also bars attempts "to control the flow of ideas to the public" as the Supreme Court ruled in *Lamont v. Postmaster General,* a case explicitly about restrictions on foreign propaganda.[6] Thus, a viewpoint neutrality standard would make it substantially more difficult for online services to police against nefarious uses of their services by foreign actors.

There is no doubt that perfectly constitutional speech has the potential to cause harm. Yet, while online services under the protection of Section 230 are imperfect guards against such harm, they have nearly infinite more power to cut off such speech than Congress. Mandating viewpoint neutrality for private online services would substantially increase the

[5] Yoo, Christopher S., What's In a Name?: Common Carriage, Social Media, and the First Amendment (October 4, 2023). U of Penn Law School, Public Law Research Paper No. 23-35, Northwestern University Law Review Online, Vol. 118, Forthcoming, Available at SSRN: https://ssrn.com/abstract=4610515 or http://dx.doi.org/10.2139/ssrn.4610515

[6] Lamont v. Postmaster General, 381 U.S. 301 (1965)

volume of the intertwined problems of harmful legal content and hostile foreign actors and leave Congress with few, if any, legal mitigation options of similar effectivity.

Section 230 is not a policy unicorn

An attack routinely leveled at Section 230 is that no other industry enjoys similar protections from civil liability. This is decidedly a canard that should be disregarded from the moment of utterance. While the federal government indeed does not commonly wade into the domain of tort law, there are plenty of examples of Congress granting civil liability immunity to various industries.

In May 2020, the Congressional Research Service (CRS) published a "Legal Sidebar" listing 13 different examples of federal tort shields across various industries and sectors.[7] Examples include liability shields for biomaterials suppliers to donors of food to charitable causes. The examples date back almost a half century all the way up to the Coronavirus Aid, Relief, and Economic Security Act (CARES) Act of 2020.

Perhaps the closest parallel to Section 230 listed in the brief is The Protection of Lawful Commerce in Arms Act. Per CRS:

> "The Protection of Lawful Commerce in Arms Act (PLCAA) prohibits plaintiffs from filing certain tort lawsuits against gun manufacturers or sellers based on the unlawful misuse of a firearm by the plaintiff or another person."[8]

The PLCAA places civil liability for the misuse of not only a lawful product, but something that enjoys explicit constitutional protections (the Second Amendment), at the feet of the (mis)user, not the producer. Regardless of the merits of such a policy, it is impossible to claim that anything about Section 230 is unique given the undeniable similarities with the civil liability treatment of firearms.

Conclusion

While the online world is undoubtedly imperfect, Section 230 walks a tightrope of massively improving the average user's online experience, broadly applying to individuals and entities of all forms and sizes in the online ecosystem, respecting property rights, and falling within the constraints of the First Amendment. Even minor shifts threaten one or more of these criteria. Section 230 is best left alone while Congress pursues other avenues to improve the state of the internet, such as enhanced resources for law enforcement and data security legislation.[9]

Sincerely,

Patrick Hedger
Executive Director

[7] Lewis, Kevin M., "Federal Legislation Shielding Businesses and Individuals from Tort Liability: A Legal and Historical Overview," Congressional Research Service, May 8, 2020. https://crsreports.congress.gov/product/pdf/LSB/LSB10461
[8] Ibid.
[9] Mohr-Ramirez, Michael, "Bill of the Month: Invest in Child Safety Act," Taxpayers Protection Alliance, January 31, 2024. https://www.protectingtaxpayers.org/congress/bill-of-the-month-invest-in-child-safety-act/

April 10, 2024

Chair Cathy McMorris Rodgers
House Committee on Energy and Commerce
Washington, DC 20515

Ranking Member Frank Pallone
House Committee on Energy and Commerce
Washington, DC 20515

Chair Bob Lotta
Subcommittee on Communications and Technology
Washington, DC 20515

Ranking Member Doris Matsui
Subcommittee on Communications and Technology
Washington, DC 20515

Dear Chairs Rodgers and Lotta and Ranking Members Pallone and Matsui,

Thank you for the opportunity to provide input ahead of the Thursday, April 11 hearing "Where Are We Now: Section 230 of the Communications Decency Act of 1996" being held by the House Energy and Commerce Subcommittee on Communications and Technology. Engine is a non-profit technology policy, research, and advocacy organization that bridges the gap between policymakers and startups. Engine works with government and a community of thousands of high-technology, growth-oriented startups across the nation to support a policy environment conducive to technology entrepreneurship.

Intermediary liability frameworks, including Section 230, are incredibly important to startups that host a wide variety of user-generated content—comments, reviews, question-and-answers, messages, photos, videos, and more—but do not have the resources of their large competitors to constantly navigate expensive litigation or even the threat of litigation any time one user is unhappy with another user's content or with a platform's content moderation decisions. The average seed-stage startup (already a relatively successful startup that has attracted outside funding) has about $55,000 per month to cover all of its costs.[1] Even one lawsuit over user-generated content that makes it to the motion to dismiss stage could wipe out a startup's entire budget for the month. At the same time, startups already spend significant amounts of time and money on content moderation to keep their platforms safe, healthy, and relevant for their users. (See Appendix A, Engine's "Startups, Content Moderation & Section 230" report.)

While many Section 230 policy debates center on the largest Internet platforms, companies of all sizes—especially startups—are empowered by Section 230 to host, moderate, and remove content in the ways that make the most sense for them and their community of users without the fear of ruinous litigation. Conversations about potential changes to foundational Internet intermediary liability frameworks should include the perspective of startups that navigate the

[1] The State of the Startup Ecosystem, Engine (April 2021) https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/60819983b7f8be1a2a99972d/1619106194054/T he+State+of+the+Startup+Ecosystem.pdf.

already expensive and time consuming task of hosting and moderating user content. (See Appendix B, Engine's "Startup Spotlight on Content Moderation".)

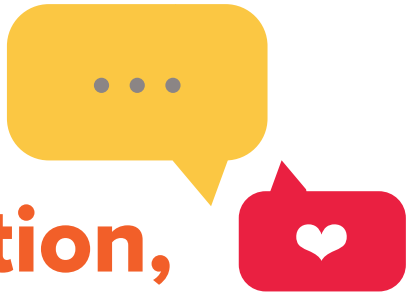
We hope the committee finds this information helpful as you explore the role of Section 230 in the Internet ecosystem. Section 230 is critical for startups, and we are available to be a resource for the committee on these issues.

Sincerely,

Engine

Appendix A

Startups, Content Moderation, & Section 230



Engine

Debates about the intermediary liability framework provided by Section 230 have animated policy conversations as lawmakers grapple with harmful online content, including around election integrity, health information, and children's safety. But those debates are almost exclusively focused on the largest Internet companies. Section 230, however, applies to all services of all sizes that host all types of user-generated content, including startups.

Section 230 helps startups avoid being inundated with lawsuits over their users' speech and limits potentially-ruinous legal costs. Startups still have incentives to invest their limited time and resources in content moderation, including, for example, to ensure that content appearing on their site is useful and relevant to their users or within their terms of service. In fact, Section 230 ensures they won't be held liable for users' speech even though they're active moderators. Despite startups' efforts, content moderation is inherently imperfect. Placing even higher, unrealistic expectations on startups—such as opening the door to lawsuits when a startup inevitably fails to perfectly and immediately remove harmful content—could take content moderation costs from burdensome to catastrophic, or even push startups to avoid hosting user content entirely.

To better understand how startups moderate content on their services, how that differs from mid-sized online service providers, and the value of Section 230 for startups, we surveyed and had conversations with user content-hosting startups in the Engine network, mid-size online service providers, and attorneys that work on 230-related cases. (We originally released a document on the costs of 230-related litigation in 2019. We confirmed that the figures below are accurate as of 2021.) As the responses show, startups have limited resources to moderate content on their sites, but they spend more per user than mid-sized content-hosting companies. And, even with Section 230 in place, defending against lawsuits involving user speech online can quickly become expensive.

Startups & Content Moderation

Startups monitor and moderate content on their sites because they recognize the potential for problematic content to appear that might contradict their values, undermine the trust of their other users, or threaten their ability to grow. Most of the startups we spoke with do not yet encounter problematic content at a rate that requires a large moderation team or expensive, sophisticated moderation technology. However, as startups scale, they begin to encounter more content requiring their attention.

The startups we spoke with each enable or host user-generated content, but they do not have the same business models as one another. The companies are between 2 and 7 years old, generate less than $100,000 in annual revenue, have fewer than 10 employees, and serve between 1,000-5,000 monthly active users. Each of the companies had raised $50,000 or less in publicly-announced funding through grants, pitch competitions, crowdfunding, and small, formal funding rounds—except one company that had raised $100,000 or less.

The responses reveal that it is critical for startups to have the ability to moderate content on their services as they see fit according to their specific size and need. Thanks to the varying need and resources put toward moderation at the current point in their lifecycle, the cost per user of each startups' moderation efforts ranged from a few dollars to over $150 per user.

Startups spend thousands of dollars on human content moderation

For most of the startups we surveyed, moderation is conducted by humans, on an as-needed, case-by-case basis. Moderation did not comprise any startup employee's entire job, mostly due to scale. If they allocated resources toward it, companies spent up to $10,000 annually on training for the employees moderating content.

Startups spend tens, or even hundreds, of thousands of dollars on content moderation technology

Most of the companies we spoke with did not use technology as part of their moderation processes, because moderation technologies were unwarranted due to scale, were prohibitively expensive, and are ultimately imperfect, requiring human review as a backstop. As one startup founder noted in discussing the costs of content filtering technology, if its use were required by law, "it would put us out of business." However, most of them plan to use technology to assist moderation efforts in the future, as warranted by scale.

For the companies that do currently use technology, the amount they had spent over the company's lifetime developing their technology varied widely, from $40,000 all the way up to $1,000,000. Those startups spent up to $50,000 annually maintaining their proprietary technology.

Some startups license technology that is developed by others to support moderation efforts on their sites, but it does not make for a low-cost alternative to developing moderation technology in-house. Licenses for software used by the startups we spoke with can cost up to $10,000 annually, and licensed software must be integrated into their service, which can be a one-time expense of up to $10,000.

Mid-Sized OSPs & Content Moderation

As user-content hosting companies scale, the amount of user-generated content that must be moderated grows. Mid-size online service providers (OSPs) have standard processes, dedicated staff, and licensed and proprietary technologies to help moderate content on their sites.

The mid-size OSPs we spoke with are between 11 and 15 years old, generate more than $50 million to more than a billion dollars in annual revenue, employ 100 to 5000, and serve almost a million to just under a half-billion monthly active users. Like the startups we spoke with, they each enable or host user content but have varying business models.

The OSPs' responses underscore the investments they make in moderating content on their sites. While they spend much larger sums on moderators and moderation software than startups, thanks to economies of scale, their cost of moderation on a per-user basis is lower. As shown in similar research, the companies' per-user moderation costs ranged from as little as a number of cents to a few dollars.

Mid-sized OSPs spend millions on human content moderation

All of the OSPs we spoke with employ human content moderators, and just one of the companies have moderators where moderation is not their only job responsibility. The companies employ up to 250 human moderators, with most OSPs employing fewer than 50 moderators. Over half of the OSPs utilized external contractors as moderators. Most of the OSPs spent between $1,000,000 and $5,000,000 annually to retain their moderators, who tend to stay at the company between 1 and 3 years. The companies spend up to a quarter of a million dollars training and equipping their moderators annually.

In the course of moderating content on their services, OSPs' trust and safety teams responsible for moderating content often collaborate with other departments at the company like legal, policy, and public relations. These cross-company collaborations often follow controversial or high-profile moderation decisions and could represent up to 10,000 work hours annually, the full cost of which is difficult to estimate given the varying salaries and opportunity costs implicated.

Mid-sized OSPs spend millions, or even tens of millions, of dollars on content moderation technology

To support their human moderators, the OSPs each utilize proprietary technologies they've developed, and some additionally license moderation technology. The companies spent between $500,000 and $30,000,000 developing their proprietary moderation tools. That development involved a similarly wide range of estimated engineering work hours—between 500 and 300,000. Companies spent between $1,000,000 and $5,000,000 to maintain their proprietary tools on the high end, and less than $250,000 on the low end.

Companies annual spending on licensing moderation tools similarly ranged between $1,000,000 and $5,000,000 on the high end, and less than $250,000 on the low end. For most OSPs, integrating the licensed technology required fewer than 200 engineering work hours and cost less than $50,000. One company spent over $2,000,000 integrating licensed technology, requiring nearly 2,000 engineering work hours.

Section 230 & Litigation Costs

Section 230 of the Communications Decency Act is often credited with the creation of the modern Internet by enabling a diverse, vast spectrum of Internet companies to host user-generated content. The law was created after court cases in the 1990s extended traditional distributor liability frameworks to Internet companies that did not moderate content on their sites but found Internet companies that engaged in any moderation to be liable for all of the content they hosted, effectively creating a disincentive to engage in moderation.

The law has two key provisions: The first ensures that Internet companies cannot be held liable for content created by their users. The second ensures that liability limitation applies even if a company engages in moderation "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."

Taken as a whole, the law gives companies the needed certainty to host user-generated content by helping to quickly dismiss cases when one user wants to sue over the content another user has created. This is especially important for startups that host user-generated content like comments, photos, classified listings, and more, enabling them to operate when they might otherwise be quickly overrun by costly lawsuits or even threats of costly lawsuits.

But even with Section 230, however, frivolous lawsuits can still pose crippling costs for startups. Section 230 does not deter all lawsuits—meritorious or not—and defending them can be especially expensive and burdening for startups, even under the current law. The value of Section 230 is that Internet companies can use it as a clear-cut affirmative defense early on in the litigation process, which helps avoid legal expenses that pile up as litigation progresses.

Pre-complaint: $0 to $3,000: Threats of litigation can present costs to startups even before a lawsuit is filed. Responding to a threatening demand letter based on user speech can carry legal costs of up to $3,000. Startups have strong incentives to resolve disputes before they turn into lawsuits, given the legal and potential reputational costs of defending an even meritless suit. Parties sending such letters are likely to know their claims lack merit because of Section 230, and are typically seeking to extract a nuisance-value settlement.

Beyond offering a response, receiving a demand letter creates additional burdens for startups as well. If a company believes a lawsuit is likely, they are obligated to issue a litigation hold and preserve documents and information that may be related to the case. A litigation hold can be burdensome and distracting for startups with limited resources.

Motion to dismiss: $15,000 - $80,000: Filing a motion to dismiss is a startup's first opportunity to end a lawsuit once one is filed. In the motion, a startup must show that it is not liable for the speech at issue, even if the plaintiff's claims are true. If the plaintiff alleges a user posted the content at issue in the lawsuit, the startup is likely to be successful dismissing the lawsuit on Section 230 grounds, since the law establishes the startup is not liable for user speech it did not create. However, that does not mean the lawsuit did not burden the startup. A motion to dismiss generally carries a cost between $15,000 and $40,000 but could go as high as $80,000. That is nearly a month of operating resources for the average seed-stage startup—meaning a meritless lawsuit could deplete an entire month's worth of a startup's resources. And the average seed-stage startup is already relatively successful and well-resourced, considering how few startups receive that kind of outside funding. For many of the startups we spoke with, that could consume their entire funding to date. Beyond these costs, plaintiffs are generally allowed the opportunity to amend their claim, meaning an intentionally-deceitful plaintiff could amend its complaint to allege the startup did create the content at issue, allowing the case to proceed and creating future legal costs for the startup.

Early Motion for Summary Judgment: $15,000 - $150,000+: Parties can file a motion for summary judgment when there are undisputed facts upon which the court can decide the case without the need for a full trial. A startup might file an early motion for summary judgment in cases where the outcome rests on a few factual questions, such as who is responsible for content posted online. Filing such a motion generally involves minimal discovery, limited to information about the user's identity and the role of the startup in creating the content at issue, but can still create legal costs around $30,000. In addition to those costs, preparing and filing the motion can cost between $30,000 and $70,000.

While some attorneys prefer to file an early motion for summary judgment rather than a motion to dismiss—because courts rarely grant the motion without giving the plaintiff a chance to correct the pleading—early motions for summary judgment come with risks as well. Filing an early motion may forfeit a startup's right to file one later, since courts tend to disfavor or prohibit multiple motions for summary judgment. Failure to get a case dismissed on summary judgment means the parties must litigate through trial or settle. Both can be incredibly expensive options that deeply burden startups.

Discovery and Trial: $100,000 - $500,000+: Lawsuits against websites for user speech rarely proceed through discovery and to trial because the associated legal costs are likely to exceed potential liability. There is no fee-recovery in 230 cases, meaning each party pays their own legal fees regardless of who wins. These dynamics incentivize resource-strapped startups to settle, even if they are likely to win. Those cases that do proceed to trial, however, quickly reach six-figure costs.

Appendix B

STARTUP SPOTLIGHT ON Content Moderation

"Section 230… is the rock on which all websites that deal in user-generated content are built—they would not exist if people could sue companies for whatever their users put online. … On copyright, in order for Fiskkit to work, our users must be able to criticize the writing of others. And we, and our users, cannot and should not be limited to criticizing articles only when authors give permission. … Many media organizations, content owners, and authors have infinite legal budgets—and even if they don't, the cost to file a case is small but the risk of our losing is enormous—a small company like Fiskkit could be broken by even the threat or filing of a meritless copyright case over acceptable fair uses." - **John Pettus**, Founder of San Francisco-based **Fiskkit**

"If [Section 230] were to change, it would cause a lot of angst and unnecessary cost, which we don't have the resources to handle. Having to build a filtering system on the front end that would filter user content [to detect copyright infringement] would be extremely cost-prohibitive. Frankly, if that was a system we had to build on day one to get this off the ground, then we probably would never have even started." - **Andrew Prystai,** Co-Founder of Omaha-based **Event Vesta**

"We're doing this work because we saw a need to better support [mental health] direct care professionals so that they are equipped with the skills to really chart a course in their careers and stay there for the long term. If it's always coming to mind whether we could get sued because of something a user says or posts, then we're never really engaging in the core purpose of disrupting a space that needs to be disrupted." - **Yasmin Mattox,** Founder of Rochester-based **Arkatecht**

"As a newer, infant company, we haven't had to tackle scaling up content moderation systems because people aren't generating much of their own content yet, but it will become an important issue. We will need to put more safety measures in place, including tools to educate users, because if someone uploads a YouTube video to the platform, and they're not paying attention to whether or not that was acceptable or they're trying to generate revenue from it, then it will become an issue we have to manage." - **Jared Scherz**, Founder of Mount Laurel-based **TeacherCoach**

"Moderation is something we are thinking about heavily. We are still in beta testing so this is something we are still thinking through as we refine the platform and grant access to new users. … Our goal is obviously to avoid [copyright infringement] on the Tomodachi platform. The way we created the tools on Tomodachi, they are really for students to create and come up with their own original work and that is what we are celebrating." - **Na Xue,** Co-founder of Los Angeles-based **Tomodachi**

"For copyright issues we follow the rules laid out by the Digital Millennium Copyright Act (DMCA), and the structure of that system has worked well for us. … We wish that there was a similar straightforward process for trademark issues. Ideally, the DMCA would just be extended to cover alleged trademark infringements as well. It would make it much easier to run a user-generated content business." - **Christian Braun,** CEO of Superior-based **hobbyDB**

"We want companies to be paying attention to accessibility, and if we had to constantly focus on moderating content, it would stop us from growing and getting the traction that we need for big organizations of the world to take notice of us. And it would hurt us a lot if we had to deal with legal action from companies that did not like a review they got. … When that funding comes through the door we want to focus it on creating value for our customers and find new ways to bring in revenue. We do not want to have to focus that money on a defense attorney retainer." - **Brandon Winfield**, Founder of Atlanta-based **iAccess Life**

April 11, 2024

Statement for the Congressional Record – Alliance for Safe Online Pharmacies (ASOP Global)

House Committee on Energy & Commerce, Subcommittee on Communications and Technology Hearing: "Where Are We Now: Section 230 of the Communications Decency Act of 1996"

The Alliance for Safe Online Pharmacies (ASOP Global) applauds the Committee for holding this important hearing on Section 230 reform and recognizing the growing concern that the law has had unintended consequences. ASOP Global is a nonprofit organization dedicated to public health and requests that you consider raising the dangers of prescription medicines and drugs sold illegally via online during this important hearing.

The Alliance for Safe Online Pharmacies was established in 2009 to combat illegal online pharmacies and counterfeit medicines and to make the internet safer for patients worldwide through research, education, advocacy, and collaboration. ASOP Global's U.S.-based members include 30+ nonprofit groups, prescription discount programs, academic institutions, patient organizations, telehealth companies, pharmaceutical manufacturers, health care providers, pharmacy organizations, shippers, payment processors, and internet security companies. To date, U.S. policy has failed to protect Americans from illegal internet drug sellers who profit at the expense of patients' safety. This is especially concerning given that the internet and social media platforms are now more than ever relevant to patient access to care and the dissemination of public health information.

Initially meant to safeguard free speech online, the outdated protections in Section 230 of the Communications Decency Act of 1996 provide immunity from civil liability for online publishers of third-party content. With no accountability for the content published via their platforms, internet intermediaries have free reign to facilitate illegal and dangerous activity online – including the sale of the illicit and counterfeit drugs that now fuels both the spread of COVID-19 fraud and the nation's opioid crisis.

The Alliance for Safe Online Pharmacies (ASOP Global) supports targeted Section 230 reform, like the bipartisan Cooper Davis Act (S. 1080) and See Something Say Something Online Act (S. 147), to hold social media platforms accountable for illegal activity online. Of the roughly 35,000 active online pharmacies at any given time, 95% do not comply with applicable laws and pharmacy standards. These sites threaten American lives by selling medicines without a prescription, operating without a license, and peddling fake drugs, often containing dangerous — even deadly — ingredients like paint thinner, fentanyl, mercury, and tar. The rampant online

sale of illegal and fake medications is fueling both the spread of COVID-19 fraud and the nation's opioid crisis.

Thank you again for the opportunity to provide you, your staff, and the members of your committee with this information. ASOP Global recognizes you will receive countless responses from interested stakeholders and will have many interests to consider as you prepare for this hearing.

ASOP Global's positions on Section 230 reform are further detailed on our website. At the end of this letter, we have compiled a list of some examples of how online platforms have allowed illegal drug sellers to peddle illegal drugs to consumers. **We do request that you raise the issue of illegal drugs sold via online platforms during the hearing and that this letter and the accompanying examples be submitted to the hearing record on April 11.**

Should you or your staff have any questions related to illegal drug sales online and how platforms facilitate these dangerous practices, please view ASOP Global as a resource. We look forward to working with you to advance public health and patient safety. **Please visit ASOP Global's website for additional information on Internet Accountability and ASOP's previous statement applauding the Committee's work on focusing on the need for Section 230 reform.**

ASOP GLOBAL | ALLIANCE FOR SAFE ONLINE PHARMACIES

Examples of illegal online drugs

Platform	Illegal Drug Sale	Link
Google	**Tramadol:** FDA sent a warning letter stating the website operates in violation of the Food, Drug, and Cosmetic Act and was selling unapproved opioids online availablepharmacy.com is still available on Google as of 3/17/21	https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/xlpharmacy-05292018
Google	**Abortion pills:** FDA sent the operators of this website a warning letter citing Food, Drug, and Cosmetic Act violations, including the sale of misbranded and unapproved drugs goabortion.com is still available on Google as of 3/17/21	https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/rablon-1111111-03082019
Google	**Breast cancer and antiviral drugs:** FDA sent a warning letter stating the website operates in violation of the Food, Drug, and Cosmetic Act and was selling unapproved and misbranded drugs online canadianqualitydrugs.net is still available on Google as of 3/17/21	https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/icerx-1111111-10092018
Google	**Tramadol and unapproved HIV treatment drugs:** FDA sent a warning letter stating the website operates in violation of the Food, Drug, and Cosmetic Act and was selling unapproved and misbranded drugs online buymeds247online.com is still available on Google as of 3/17/21	https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/farma-glow-111111-10092018
Google	**Misbranded Oxycodone:** FDA sent a warning letter stating the website operates in violation of the Food, Drug, and Cosmetic Act and was selling unapproved and misbranded drugs online aaapharm-palace365.ru is still available on Google as of 3/17/21 and is now selling Cialis.	https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/discount-pharmacy-1111111-10092018
Facebook	**"Drugs:"** Chicago police on Tuesday announced their latest arrests for illegally selling guns and drugs through private Facebook groups Facebook claims to monitor these groups, but CPD detectives have labeled these private hidden sites as a version of the dark web that's more accessible for everyday users	https://www.chicagotribune.com/news/breaking/ct-guns-drugs-facebook-bust-20191203-vrhqb7g2hng3hasfbf7mfovcqi-story.html
Facebook	**Tramadol and Carisoprodol:** Snyder and the conspirators communicated concerning shipments of Tramadol and Carisoprodol tablets using social media, including Facebook	https://www.justice.gov/usao-mdpa/pr/snyder-county-man-charged-conspiracy-distribute-over-100000-prescription-pain-pills
Facebook	**COVID vaccines and meds:** The offers ranged from Facebook page operators willing to ship Sinovac Covid-19 vaccine—which is not authorized for use in the United States—from China, to apparent scammers on Telegram claiming to have access to Moderna, Pfizer, and AstraZeneca's vaccines	https://www.wired.com/story/covid-19-vaccine-scams-spread-facebook-telegram/
Facebook	**COVID vaccine**: Office for the Western District of Kentucky has filed a lawsuit in federal court in Louisville, Kentucky to shut down a webpage, six related web addresses and a related Facebook page that the suit says are attempting to lure consumers to "pre-register" for a non-existent COVID-19 vaccine in exchange for $100 worth of Bitcoin	https://www.justice.gov/usao-wdky/pr/us-attorney-s-office-shuts-down-multiple-websites-claiming-offer-preorders-covid-19

Facebook	**COVID products:** Herbal products, including "Carahealth Immune," which is also referred to as "Immune Tonic" on the website, for sale in the United States and that these products are intended to mitigate, prevent, treat, diagnose, or cure COVID-19	https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/carahealth-605826-03262020
Facebook and Instagram	**Counterfeit Pfizer medications:** Illegal online sales have moved from websites to social media platforms. From 2015-2018, more than 10,000 Facebook accounts selling counterfeit Pfizer medications were identified, while during a six-month period in 2018, 1,000 Instagram accounts were also reported	https://bpp.msu.edu/magazine/industry-sector-update-what-health-professionals-need-to-know/
Instagram	**Opioids**: A new study used machine learning to flag Instagram posts mentioning opioid and other illegal drug sales — and roughly 10 percent, or more than 12,000 posts were from users advertising drugs, researchers found. Buyers and sellers also discussed transactions in the comments; researchers recommended that social media platforms crack down on illegal sales on their sites	https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6598421/
Instagram	**Counterfeit steroids:** Ensuing posts included hashtags such as #steroids, #gains, and #trenhard—a reference to trenbolone, the most powerful anabolic steroid on the market. So far, though, Silicon Valley's response has been sluggish at best. The tech giants claim immunity under a law that likens social media companies to newsstands rather than to publishers responsible for the content on their platforms. In other words, they argue, social media companies don't create the offensive material that ends up on their pages, so they can't be held liable	https://www.bostonmagazine.com/health/2019/10/15/instagram-drug-market/
Facebook and Instagram / WhatsApp and WeChat	**All drugs / other products**: On Facebook and Instagram, it's common for traffickers to post their WhatsApp or WeChat numbers alongside their goods, a signal to prospective buyers to connect in a more private forum. From orangutans and cheetah cubs to opioids and ancient Middle Eastern antiquities, if something can be sold illegally, researchers say, it's likely being sold somewhere on Facebook or Instagram	https://www.bloomberg.com/news/articles/2019-07-11/wildlife-traffickers-use-facebook-instagram-to-find-black-market-buyers
Instagram, Snapchat, Facebook, Tik Tok	**Benzos**: Teen addiction to benzodiazepines, called "benzos" for short, is on the rise, and these drugs are easier for teens to access—and get addicted to—than most parents think. In fact, they can be as easy to order as direct messaging a dealer on Instagram. Even if teens do not have direct access to a prescription, finding a supplier can be as simple as logging into their social networks like Snapchat, TikTok, Facebook, and Instagram Facebook, which owns Instagram, says they are working to ensure illicit drug sales do not happen on the platform. "As our Regulated Goods policy explains, we prohibit attempts by individuals, manufacturers, and retailers to purchase, sell, or trade non-medical drugs and pharmaceutical drugs," says a Facebook spokesperson. "We also have a strict Advertising Policy and a Commerce Policy that prohibits the sale of opioids, prescription drugs, or the operation of online pharmacies without prior permission. We have proactive detection technology in place to find and remove such content before anyone sees it, we are constantly working to improve this technology to find more content, quickly."	https://www.yahoo.com/lifestyle/benzos-rising-popularity-among-teens-174946047.html
Twitter, Facebook, Instagram, Snapchat, Fortnight,	**Fentanyl:** The Fentanyl crisis and the explosion of social media in just five years has transformed drug-pushing online. In fact, those who track illicit internet drug-selling know that drug dealers from China and	https://www.dispatch.com/opinion/20191109/column-third-parties-should-monitor-online-drug-sales

YouTube, Tumblr and Reddit	within the U.S. use social media as the new street corner, concomitantly expanding their geographic, age and social reach	
Instagram and YouTube	**COVID cure:** The DOJ charged Keith Lawrence Middlebrook, 53, with soliciting investments in a company called Quantum Prevention CV Inc. (QP20) through videos on YouTube and Instagram where he said he possessed a cure for COVID-19. Middlebrook claimed he planned to sell an injectable cure for the virus and a pill that would prevent infection, the department said." The videos had more than 1 MILLION views	https://www.justice.gov/usao-cdca/pr/southland-man-arrested-federal-charges-alleging-fraudulent-investment-scheme-featuring
Instagram and Twitter	**COVID products:** The team identified more than 6 million Tweets and 200,000 Instagram posts that promoted possible scams involving COVID-19 treatments and products. The scams they found using AI ranged from dung remedies to do-it-yourself diagnostics. The team identified a total of 1,271 Tweets and 596 Instagram posts that promoted scams and passed that data to the FDA (U.S. Food and Drugs Administration)	https://newslanded.com/2020/08/31/twitter-and-instagram-being-used-to-sell-fake-covid-19-drugs-and-diagnostics-kits-study-finds/
Snapchat	**Xanax / Fentanyl / Marijuana / all drugs:** "Like yesterday, this person added me and they were selling Xanax," said an eighth grader. Drug dealers are called "plugs" on social media, sometimes using a plug emoji to describe them. Some plugs "quick add" people on Snapchat, which categorizes users by zip code. "It really can be scary, because anytime, like, you could buy it," said the eighth grader Snapchat did not provide an official response to questions	https://kutv.com/news/addicted-utah/addicted-utah-drug-dealers-find-potential-young-customers-on-snapchat-social-media
Snapchat	**Fentanyl:** In April 2020, a San Jose man faced murder charges after selling counterfeit opioid pills containing Fentanyl to an 18-year-old woman and her boyfriend via Snapchat, which caused both individuals to overdose and resulted in the young woman's death	https://www.nbcbayarea.com/news/local/sj-man-faces-murder-charge-after-woman-ods-on-fake-opioids/2272778/
Snapchat	**Fentanyl**: Berman said a drug dealer had connected with him on Snapchat and sold him a prescription drug laced with Fentanyl. Snapchat is one of the most popular apps for buying and selling drugs, because the messages automatically disappear	https://www.wdbj7.com/2021/02/24/early-years-snapchat-and-other-social-media-being-used-by-drug-dealers-to-target-kids/
Snapchat	**Fentanyl:** On February 7, Berman announced on Instagram that her "beautiful boy" had overdosed in his bedroom after purchasing fentanyl-laced Xanax from a drug dealer on Snapchat. Snapchat said it has a zero-tolerance policy for using the platform to buy or sell illegal drugs. "We are constantly improving our technological capabilities to detect drug-delated activity so that we can intervene proactively," the company said in a statement. "We had no higher priority than keeping Snapchat a safe environment and we will continue to invest in protecting our community."	https://www.today.com/parents/dr-laura-berman-tested-son-drugs-fentanyl-death-t209764
Social Media (general)	**Xanax, Valium, Hydrocodone, Oxycodone, Percocet, and Adderall:** A fair number of the dealers that we catch in this county are young people. They advertise on social media. You have a 20-year-old-dealer, and he is going to know 18-year-old students. The word gets out, these young people drive, they do deliveries	https://sanfrancisco.cbslocal.com/2019/10/24/fentanyl-deaths-counterfeit-pills-invading-bay-area-schools/
Online (general)	**Phenibut:** It "is relatively easy to access online, but it has some pretty serious outcomes," Graves said. "It also seems to be growing in popularity, maybe even more so with the pandemic and people seeking out substances online to help with their stress."	https://news.wsu.edu/2020/09/03/poison-centers-report-big-increase-calls-phenibut/

Teen Girls Confront an Epidemic of Deepfake Nudes in Schools

Using artificial intelligence, middle and high school students have fabricated explicit images of female classmates and shared the doctored pictures.

After boys at Francesca Mani's high school fabricated and shared explicit images of girls last year, she and her mother, Dorota, began urging schools and legislators to enact tough safeguards. Credit...Shuran Huang

By Natasha Singer

Natasha Singer has covered student privacy for The Times since 2013. She reported this story from Westfield, N.J.

- April 8, 2024

Westfield Public Schools held a regular board meeting in late March at the local high school, a red brick complex in Westfield, N.J., with a scoreboard outside proudly welcoming visitors to the "Home of the Blue Devils" sports teams.

But it was not business as usual for Dorota Mani.

In October, some 10th-grade girls at Westfield High School — including Ms. Mani's 14-year-old daughter, Francesca — alerted administrators that boys in their class had used artificial intelligence software to fabricate sexually explicit images of them and were circulating the faked pictures. Five months later, the Manis and other families say, the district has done little to publicly address the doctored images or update school policies to hinder exploitative A.I. use.

"It seems as though the Westfield High School administration and the district are engaging in a master class of making this incident vanish into thin air," Ms. Mani, the founder of a local preschool, admonished board members during the meeting.
In a statement, the school district said it had opened an "immediate investigation" upon learning about the incident, had immediately notified and consulted with the police, and had provided group counseling to the sophomore class.

Image

Tenth-grade girls at Westfield High School in New Jersey learned last fall that male classmates had fabricated sexually explicit images of them and shared them.Credit...Peter K. Afriyie/Associated Press

“All school districts are grappling with the challenges and impact of artificial intelligence and other technology available to students at any time and anywhere,” Raymond González, the superintendent of Westfield Public Schools, said in the statement.

Blindsided last year by the sudden popularity of A.I.-powered chatbots like ChatGPT, schools across the United States scurried to contain the text-generating bots in an effort to forestall student cheating. Now a more alarming A.I. image-generating phenomenon is shaking schools.

Boys in several states have used widely available “nudification” apps to pervert real, identifiable photos of their clothed female classmates, shown attending events like school proms, into graphic, convincing-looking images of the girls with exposed A.I.-generated breasts and genitalia. In some cases, boys shared the faked images in the school lunchroom, on the school bus or through group chats on platforms like Snapchat and Instagram, according to school and police reports.

Such digitally altered images — known as “deepfakes” or “deepnudes” — can have devastating consequences. Child sexual exploitation experts say the use of nonconsensual, A.I.-generated images to harass, humiliate and bully young women can harm their mental health, reputations and physical safety as well as pose risks to their

college and career prospects. Last month, the Federal Bureau of Investigation warned that it is illegal to distribute computer-generated child sexual abuse material, including realistic-looking A.I.-generated images of identifiable minors engaging in sexually explicit conduct.

Yet the student use of exploitative A.I. apps in schools is so new that some districts seem less prepared to address it than others. That can make safeguards precarious for students.

“This phenomenon has come on very suddenly and may be catching a lot of school districts unprepared and unsure what to do,” said Riana Pfefferkorn, a research scholar at the Stanford Internet Observatory, who writes about legal issues related to computer-generated child sexual abuse imagery.

At Issaquah High School near Seattle last fall, a police detective investigating complaints from parents about explicit A.I.-generated images of their 14- and 15-year-old daughters asked an assistant principal why the school had not reported the incident to the police, according to a report from the Issaquah Police Department. The school official then asked “what was she supposed to report,” the police document said, prompting the detective to inform her that schools are required by law to report sexual abuse, including possible child sexual abuse material. The school subsequently reported the incident to Child Protective Services, the police report said. (The New York Times obtained the police report through a public-records request.)

In a statement, the Issaquah School District said it had talked with students, families and the police as part of its investigation into the deepfakes. The district also “shared our empathy,” the statement said, and provided support to students who were affected.

The statement added that the district had reported the “fake, artificial-intelligence-generated images to Child Protective Services out of an abundance of caution,” noting that “per our legal team, we are not required to report fake images to the police.”

At Beverly Vista Middle School in Beverly Hills, Calif., administrators contacted the police in February after learning that five boys had created and shared A.I.-generated explicit images of female classmates. Two weeks later, the school board approved the expulsion of five students, according to district documents. (The district said California’s education code prohibited it from confirming whether the expelled students were the students who had manufactured the images.)

Michael Bregy, superintendent of the Beverly Hills Unified School District, said he and other school leaders wanted to set a national precedent that schools must not permit pupils to create and circulate sexually explicit images of their peers.

“That’s extreme bullying when it comes to schools,” Dr. Bregy said, noting that the explicit images were “disturbing and violative” to girls and their families. “It’s something we will absolutely not tolerate here.”

Image

Michael Bregy, superintendent of Beverly Hills schools, said he wanted to send a message that schools must not allow pupils to make and share explicit images of their peers.Credit...Tracy Nguyen for The New York Times

Schools in the small, affluent communities of Beverly Hills and Westfield were among the first to publicly acknowledge deepfake incidents. The details of the cases — described in district communications with parents, school board meetings, legislative hearings and court filings — illustrate the variability of school responses.

The Westfield incident began last summer when a male high school student asked to friend a 15-year-old female classmate on Instagram who had a private account, according to a lawsuit against the boy and his parents brought by the young woman and her family. (The Manis said they are not involved with the lawsuit.)

After she accepted the request, the male student copied photos of her and several other female schoolmates from their social media accounts, court documents say. Then he used an A.I. app to fabricate sexually explicit, "fully identifiable" images of the girls and shared them with schoolmates via a Snapchat group, court documents say.

Westfield High began to investigate in late October. While administrators quietly took some boys aside to question them, Francesca Mani said, they called her and other 10th-grade girls who had been subjected to the deepfakes to the school office by announcing their names over the school intercom.

That week, Mary Asfendis, the principal of Westfield High, sent an email to parents alerting them to "a situation that resulted in widespread misinformation." The email

went on to describe the deepfakes as a “very serious incident.” It also said that, despite student concern about possible image-sharing, the school believed that “any created images have been deleted and are not being circulated.”

Image

Subject: Important Message from WHS Principal Asfendis

Good afternoon,

I am writing to make you aware of a situation that resulted in widespread misinformation and resulted in significant worry and concern amongst the student body of Westfield High School. Earlier today, students brought to our attention that some of our students had used Artificial Intelligence to create pornographic images from original photos. There was a great deal of concern about who had images created of them and if they were shared. At this time, we believe that any created images have been deleted and are not being circulated. This is a very serious incident. We are continuing to investigate and will inform individuals and families of students involved once the investigation is complete. This will happen before the weekend. We made counseling available for all affected students and encouraged them to return to class when they felt able to do so. Additionally, our School Resource Officer and the Westfield PD have been made aware of our investigation. If a parent/guardian thinks their child is a victim of a criminal act in relation to this incident please report the matter to Westfield Police.

I wanted to make you aware of the situation, as, in addition to harming the students involved and disrupting the school day, it is critically important to talk with your children about their use of technology and what they are posting, saving and sharing on social media. New technologies have made it possible to falsify images and students need to know the impact and damage those actions can cause to others.

We will continue to educate your children on the importance of responsible use of technology and hope you reinforce these messages at home.

Mary Asfendis
Principal
Westfield High School

An October email that the principal of Westfield High sent to parents about the deepfakes.

Dorota Mani said Westfield administrators had told her that the district suspended the male student accused of fabricating the images for one or two days.

Soon after, she and her daughter began publicly speaking out about the incident, urging school districts, state lawmakers and Congress to enact laws and policies specifically prohibiting explicit deepfakes.

“We have to start updating our school policy,” Francesca Mani, now 15, said in a recent interview. “Because if the school had A.I. policies, then students like me would have been protected.”

Parents including Dorota Mani also lodged harassment complaints with Westfield High last fall over the explicit images. During the March meeting, however, Ms. Mani told school board members that the high school had yet to provide parents with an official report on the incident.

Westfield Public Schools said it could not comment on any disciplinary actions for reasons of student confidentiality. In a statement, Dr. González, the superintendent, said the district was strengthening its efforts “by educating our students and establishing clear guidelines to ensure that these new technologies are used responsibly.”

Beverly Hills schools have taken a stauncher public stance.

When administrators learned in February that eighth-grade boys at Beverly Vista Middle School had created explicit images of 12- and 13-year-old female classmates, they quickly sent a message — subject line: “Appalling Misuse of Artificial Intelligence”

— to all district parents, staff, and middle and high school students. The message urged community members to share information with the school to help ensure that students' "disturbing and inappropriate" use of A.I. "stops immediately."

Image

B

Appalling Misuse of Artificial Intelligence

BHUSD Superintendent - Dr. Bregy • a month ago • Thursday, Feb 22 at 3:54 PM • **Beverly Hills High School, Beverly Vista Middle School**

Dear BVMS Community,

In the interest of full transparency, this message is being sent to all staff and parents in BHUSD as well as BHHS and BVMS students. This is an important message for our entire community.

On Wednesday, the BVMS Administration received reports from students about the creation and dissemination by other students of Artificial Intelligence generated (AI) images that superimposed the faces of our students onto AI-generated nude bodies. As the investigation is progressing today, more victims are being identified. We are taking every measure to support those affected and to prevent any further incidents.

We want to make it unequivocally clear that this behavior is unacceptable and does not reflect the values of our school community. Although we are aware of similar situations occurring all over the nation, we must act now. This behavior rises to a level that requires the entire community to work in partnership to ensure it stops immediately.

Artificial Intelligence (AI) image generation is a technology that uses machine learning algorithms to create or manipulate digital images. In this context, it has been used inappropriately to create images that are not only unethical but deeply concerning.

This emerging technology is becoming more and more accessible to individuals of all ages. We are appalled by any misuse of AI and must protect the most vulnerable members of society, our children. Parents, please partner with us and speak with your children about this dangerous behavior. Students, please talk to your friends about how disturbing and inappropriate this manipulation of images is.

While the law is still catching up with the rapid advancement of technology and such acts may not yet be classified as a crime, we are working closely with the Beverly Hills Police Department throughout this investigation. We assure you that if any criminal offenses are discovered, they will be addressed to the fullest extent possible.

Collectively, we are nothing short of outraged by this behavior and we are prepared to implement the most severe disciplinary actions allowable under California Education Code. **Any student found to be creating, disseminating, or in possession of AI-generated images of this nature will face disciplinary actions, including, but not limited to, a recommendation for expulsion.**

A February message that school administrators in Beverly Hills, Calif., sent to parents and students about deepfakes.

It also warned that the district was prepared to institute severe punishment. "Any student found to be creating, disseminating, or in possession of AI-generated images of this nature will face disciplinary actions," including a recommendation for expulsion, the message said.

Dr. Bregy, the superintendent, said schools and lawmakers needed to act quickly because the abuse of A.I. was making students feel unsafe in schools.

"You hear a lot about physical safety in schools," he said. "But what you're not hearing about is this invasion of students' personal, emotional safety."