Questions for the Record from Senator Alex Padilla
Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law
"Platform Accountability: Gonzalez and Reform"
March 8, 2023

Questions for Mr. Andrew Sullivan

1. How does Section 230 enable online interactivity?

Response: "The Internet" is really just a word for all the tens of thousands of interconnected networks in the world. These networks are each independently operated. Some of them are access networks, such as what we use when we connect to the Internet via our Internet Service Provider (ISP). Some of them provide services, such as a hosting company that provides technical services to people who put up web pages or run email servers or so forth. Still others ensure content is widely dispersed and easily available—so-called content distribution networks (CDNs). Yet others provide access to services they offer, such as the networks operated by companies like Google and Meta. Many networks include multiple parts of all of these functions. All of these differing entities are included in the scope of Section 230's definition of "interactive computer service," and all are thus protected by Section 230.

What Section 230 does is make sure that all those different operators of online services do not become liable if somebody else online says something nasty or unlawful. In that sense, Section 230 is quite literally a necessary condition to having online interactivity at all. Imagine a world in which, every time somebody said something potentially libelous, every one of the possibly hundreds of companies involved in carrying that speech act over the Internet potentially becomes another defendant in a lawsuit. Any one of those intermediaries could decide to block access to that speech rather than risk a lawsuit. Section 230 contains the recognition that, in an online context, the party that is responsible for particular content is *the party that created it*, and nobody else.

In addition to reducing legal risk to online service providers that would arise from hosting or transmitting users' content (discussed more in response to question 2), Section 230 also provides direct protection to online users themselves to forward, "retweet," or "like" content to other users. Thus, under Section 230, if a social media user sees an interesting news article and brings it to the attention of friends and family, that user will not be liable if the article is later held to be defamatory of someone. This type of online person-to-person interactivity happens literally tens of millions (if not hundreds of millions) of times every day, and it is Section 230 that allows users to engage in this online discourse and exchange of ideas without taking on significant legal risks.

2. During the hearing as well as during the Supreme Court oral argument in *Google v. Gonzalez*, some argued that simply because a company may not have immunity from suit for a particular piece of content it chooses to host, does not mean that it can be found liable for that content. In other words, lack of immunity does not automatically mean liability, which should minimize concerns about limiting the scope of Section 230 protection either via statutory interpretation or legislative amendment. **What are your thoughts on this line of argument?**

Response: It is certainly true that a lack of immunity for hosting some content does not automatically imply liability for that content. But that argument misses one of the primary—and absolutely essential—benefits of Section 230: it provides online service providers (and in the case of start-ups, their investors) with confidence that legal risks and legal costs can be controlled and minimized. Without that confidence, the prospect of hosting or transmitting the content created by hundreds of millions of users (and being potentially liable for whatever is in that content) would certainly discourage rational businesses from providing the services in the first place.

The danger to every service online—especially the hundreds of thousands of startups, small and medium sized companies, and non-profits that do not have the same resources as incumbents—lies not merely in avoiding eventual liability. Defending against a lawsuit costs money—sometimes, a lot of money—and if every claim of liability needs to be litigated in order to determine whether a party is liable, some parties will have a choice: either they will spend a lot of money defending themselves against lawsuits, or else they will restrict the ability of others to post content within sites controlled by the party in question. In other words, if I am a social media operator facing liability for posted content, it would be irrational for me not to constrict who may post and what they may say in the social media site I operate. Even if I think that I will eventually be vindicated as not liable, there is a good chance I will not want to (or cannot afford to) defend against every lawsuit anyone might think to bring.

This is especially true of new entrants to the market. It could be true that successful, well-established players would be able to afford the litigation costs. But a recent entrant will not have the financial muscle to withstand a large number of suits. Removing the protections of Section 230 would likely have the perverse effect of entrenching even more than they already are the largest tech companies. Moreover, it would quite likely cause damage to actors on the Internet that have little if anything to do with the actual speech in question (as discussed more fully in response to question 5).

In his article entitled "Why Section 230 Is Better Than the First Amendment,"[1] Professor Eric Goldman details the critical *procedural* benefits of Section 230 that enable online actors to reduce risks of high litigation costs, including allowing early dismissal of claims, greater predictability, reduction of creative drafting of claims, and avoidance of state conflict of laws questions.[2] To attempt to quantify the financial risks that startup companies might face, Engine (a non-profit advocacy organization that supports technology entrepreneurship), researched litigation costs, and concluded in 2021 that *even with Section 230 protections* a startup would likely face $15,000 to 40,000 in legal costs to defend a single lawsuit about online content, and without Section 230 costs would likely exceed $100,000 or much more.[3] When even some of today's largest online platforms are struggling to make a profit, the ability of online startups that host user content to survive without Section 230 is very doubtful.

At the hearing, some articulated the view that it would be healthy to encourage more lawsuits against online entities. Whether or not that is true for the very large and dominant online platforms, that view would be devastating for the broader Internet ecosystem. This is especially true in the United States, which is one of the few countries in the world that does not have a "loser pays" system for litigation. It costs very little to initiate a lawsuit in the U.S., but as detailed above the cost to defend even a frivolous suit can be significant. Section 230 protects hundreds of millions of ordinary Americans, plus tens (or hundreds) of thousands of small businesses, churches, non-profit organizations, and others, and the vast majority of those protected by Section 230 could be grievously harmed if Congress were to open the litigation floodgates aimed at the Internet.

Moreover, apart from legal and financial risks posed to small businesses and others, Congressional action that increases the risk of litigation over online content would certainly lead to the suppression of speech online. In many cases—even frivolous cases—the defendant company would have no practical choice but to agree to remove or block the content targeted in the lawsuit. Even for larger companies, it often is simply not worth the cost of litigation to defend a piece of speech posted by a customer. This would create a powerful 'heckler's veto' that bad actors could exploit: any speech by disfavored minorities, or that is at all controversial in our society, or that any segment of our society might want to suppress, would be at risk of suppression simply because it does not make business sense for a company to pay tens or hundreds of thousands of dollars to fight to keep a particular piece of content online.

---

[1] Goldman, Eric, *Why Section 230 Is Better Than the First Amendment*, Notre Dame Law Review, Vol. 95, No. 33, 2019, available at SSRN: https://ssrn.com/abstract=3351323 or http://dx.doi.org/10.2139/ssrn.3351323.

[2] *Id*. at 39-44.

[3] Engine, *Startups, Content Moderation, and Section 230* (2021), available at https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/61b26e51cdb21375a31d312f/1639083602320/Startups%2C+Content+Moderation%2C+and+Section+230+2021.pdf.

3. As the title of the hearing properly alludes to, there's a lot of Congressional and public interest in ensuring that we have a legal and regulatory environment that enables consumers and regulators to hold companies accountable for their own harmful conduct.

    a. **Under existing Section 230 caselaw such as the 2008 Ninth Circuit decision in *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC* and recent Fourth Circuit decision in *Tyrone Henderson, Sr. v. The Source for Public Data, L.P.*, how can platforms be held accountable for their own conduct?**

Response: Section 230 does not protect against liability for *every* action. Instead, it protects intermediaries and users from liability for *content posted by others*.

If an intermediary's own intentional actions create a harm that is independent of any harm that might be caused by content provided by others, to a non-lawyer (like me) that would appear to be outside of the protection of Section 230. Thus, as alleged in *Roommates.com*, if the website questions created by a roommate matching service themselves violate a federal housing statute, then Section 230 would not apply. If, as apparently alleged in the *Henderson* case, the defendant created and published its "own internally created summaries" of criminal charges, then again it would seem that Section 230 would not apply to such summaries (but that case is still in active litigation, differing federal judges disagreed, and we have not looked closely at the underlying court papers, and so we don't have a position on whether that particular decision was correct). Similarly, beyond those two examples, if a company intentionally chooses to display content in a discriminatory manner based on a legally protected class—such as the race of the site visitor—that also would appear to be outside of Section 230.

One important distinction to make is that some "actions" of online intermediaries are—and should be—protected by Section 230 (and I understand also likely protected by the First Amendment). Section 230 expressly protects decisions by an online intermediary to organize, select, and display content submitted by users, and most online sites could not function without protection for the actions of organizing, selecting, and displaying content. That activity is exactly what Congress in the mid-1990s had the foresight to understand would necessarily be done by computer programs rather than humans, and for the Internet to function as a useful information access system, such organization and display of content must be protected.

b. What tools are available to consumers and regulators to hold platforms accountable for their own harmful conduct?

Response: The answer to this question depends on the nature of the harm and the nature of the accountability desired. For instance, Section 230 already does not protect anyone from federal criminal liability when crimes are committed. In the *Gonzalez* case, the United States could have brought charges against the service provider if it concluded that the provider acted unlawfully. It is possible that some of the things Congress wishes to control could be criminal offenses, and Section 230 would offer no protection there.

In addition, some of the issues that get blamed on Section 230 are actually other kinds of failures. For instance, many Americans understandably express concern about tracking and targeting of information or advertising. Yet comprehensive privacy legislation would tackle such issues more directly, by allowing people to avoid or control such tracking in the first place. That in turn would give users much greater control over what information online services can use to target content and advertisements. Similarly, some concerns about the harms from platforms are really rooted in concerns about corporate size and influence—a problem in no way confined to tech platforms.

More broadly, as my initially testimony addressed on pages 5-6, Section 230 is a very poor vehicle for Congress to use to address many of the significant concerns about content on the Internet. Because Section 230 provides essential protection to a huge diversity of service providers—most of which do not have and should not have visibility into the content of communications—carving out new categories of content that would not be covered by Section 230 will impose significant legal risk on parties that have little to no ability to address the harm identified. A new carve out of content from Section 230 would impose legal risk on, for example, the thousands of small Internet Service Providers that provide crucial Internet access in rural, minority, and other underserved areas of the United States. Although the largest ISPs in the country have large legal staffs and significant financial resources, some smaller ISPs would be threatened by even a single lawsuit enabled by reducing Section 230's protections.

4. In her testimony Professor Franks suggests that we consider amending Section 230 to limit the scope of the provision to speech as opposed to "information" by replacing the word "information" in Section 230(c)(1) with "speech." **What are your thoughts on this proposal?**

Response: It is hard to know what impact it would have, for two reasons. First, it seems likely that, at the very least, a vast array of information online is effectively conveyed by something we (and the courts) are likely to recognize as speech. So, on its face, the proposal does not seem likely to satisfy the desire to alter Section 230 in the interests of various social goals. In addition, the Supreme Court and other courts of the United States

have recognized many kinds of actions as effectively being speech anyway—perhaps most notably, spending money.

At bottom, we have not seen a sufficient explanation of the proposed change, and what exactly is included in "information" that is not included in "speech." In Professor Franks' paper in which she first proposed this wording change,[4] she included a list of online "products":

> search engines, social media, online publications with comments sections, Wikis, private message boards, matchmaking apps, job search sites, consumer review tools, digital marketplaces, Airbnb, cloud storage companies, podcast distributors, app stores, GIF clearinghouses, crowdsourced funding platforms, chat tools, email newsletters, online classifieds, video sharing venues …,

and then asserted that "many of these 'products' have very little to do with speech …."[5] But it is wholly unclear which of the listed online services do not involve speech, and in our view the great majority of them precisely involve the type of user-contributed speech that Section 230 was designed to facilitate. And for any online sites that in fact do not involve content posted online by others, such sites would not in any event be protected by Section 230.

---

[4] Franks, Mary Anne, *Reforming Section 230 and Platform Liability*, Cyber Policy Recommendations for the New Administration, STANFORD CYBER POLICY CENTER, Jan. 27, 2021, available at SSRN: https://ssrn.com/abstract=4213840 or http://dx.doi.org/10.2139/ssrn.4213840.

[5] *Id.* at 7-8. In her testimony in this hearing, Professor Franks identified a different list of activities as not being speech: "paying bills, selling stolen goods, shopping for dog leashes, booking hotel rooms, renewing driver's licenses." We could easily agree that paying an electric bill on the electric company website, or renewing a license on a government website, may not involve speech covered under Section 230, but that does not seem to support any change to the language of Section 230. On the other hand, if a maker of craft dog leashes sells them on the Etsy marketplace, the seller very likely describes the dog leashes for sale, and Etsy is likely protected from liability under Section 230 if a dog leash is misdescribed. But it is unclear how changing the statutory language of Section 230 from "information" to "speech" would impact that protection (as courts have clearly held that offering products for sale is a form of speech).

5. Congressional debates about intermediary liability reform are usually rhetorically limited to those actors that operate at application layer of the Internet. However, as you shared in your testimony, Section 230 extends to the infrastructure intermediaries below them. You highlighted in particular: Internet Service Providers, Content Delivery Networks and Web Hosting Companies.

   a. What should legislators know about the different kinds of intermediaries protected by Section 230?

Response: The rich set of networks, services, and information on the Internet is made possible by a vast set of supporting services and infrastructure, much of which operate smoothly out of the view or interest of the public or policymakers. Every single one of these elements of our online environment depend on the protections of Section 230 in their normal everyday operation. As discussed above, Section 230 amendments aimed at the application layer (which is where the major online platforms generally operate) run the risk of creating collateral damage—regulatory shrapnel, if you will—that can do grave and unknown damage to the machinery of the Internet.

On the other hand, it would not be straightforward to craft a Section 230 amendment narrowly tailored to the "application layer" of the Internet. While the idea of the application layer can in general terms be simply explained, actually deciding what is an application and what is in that layer is extraordinarily difficult. This is related to the difficulty of understanding each of the intermediaries mentioned in the question.

For instance, when you visit a web page, the web page *looks* like a single thing. This is part of the technical ingenuity of the Internet, because in fact a web page can be assembled out of many different parts, which may be provided by many different providers. To give an example, in a web page with video embedded, very often the video content is widely distributed through the use of a Content Delivery (sometimes "Distribution") Network (CDN). This is done so that everyone does not have to fetch a very large file from a single source on the Internet, because that would be slow and unsatisfying to the viewer and would increase network congestion. CDNs work well when they are completely agnostic about the content of the files they are distributing. To a CDN, every file is just a "bag of bits" to be distributed as quickly and efficiently around the Internet as possible. CDNs can act this way because they are not liable for those contents. If they became liable, they would have to examine every file and make their own determinations of their liability. This would not only slow service. It also represents the potential for corporate censorship as well as privacy violations.

In addition, the example above is for a web page that has only a single video embedded. But many web pages are much more complicated than that, with multiple different items embedded within the single web page. Each of these might be coming from a different source—perhaps the website operator, perhaps a different website, perhaps a CDN (not

necessarily the same CDN as the video), and so forth. All of this happens in milliseconds, so that your visit to the web page works exactly as you expect it to. But every one of those sources that make up the web page you are visiting are protected by Section 230.

Similarly, Internet Service Providers (ISPs) and Web Hosting Companies also rely on the same intermediary liability protections. It would be impossible for a large web host, for instance, to know all the content posted on machines they are operating. Imposing such liability would dramatically disrupt and threaten the current functioning of the Internet.

Moreover, it is not only liability protection from content posted by others that intermediaries get in Section 230. They *also* get protection from liability for their good faith efforts to manage problems that they see on their platforms. For instance, many concerns about Section 230 protections focus on the items that platforms do not remove from their systems. But equally vexing are cases where platforms remove content that may turn out not to be a problem, but that they believe to be dangerous due to automated content monitoring and so forth. Protecting such well-meaning activities from liability is *also* important, because it enables the very kinds of content moderation that some in society think platforms should do more aggressively.

b. How should these differences inform proposals to amend Section 230?

Response: The reality is that actually amending Section 230 would be devilishly hard to do. Because the Internet is made of so many different pieces, even describing all the relevant parties in legislation is difficult—and that is before we recognize that some kinds of entities and services might not have been invented yet. This is exactly what is at stake: the Internet was designed to be built upon, and is constantly evolving and changing. It is a tool of creativity and innovation, and Section 230—which used broad statutory categories to allow evolution—is essential to enabling that innovation.

That is, part of what has made the Internet so important is that it is itself an environment of innovation. Even the large platforms present a home for such innovation, where people find ways to address social ills. Plenty of addicts have found their way to recovery through Google searches or Facebook friends. Many at-risk youths in communities facing disproportionate rates of suicide are alive today because they found help and made connections with peers through outreach campaigns like We Matter on platforms like Facebook and YouTube. News that is important to a widely-dispersed community of people, and that would never have been reported in traditional media, becomes an opportunity to create community online. Political viewpoints—whether left, right, or center—that were once too small to form communities at all can now debate and work out political programs as part of the great American tradition of public debate. Medical miracles that once had to spread at the speed of journal articles and postal mail can now happen because scientists collaborate, sometimes even in real time, with their earliest

scientific results. Experts in medicine, agriculture and other disciplines can advise remote communities over the Internet. People cheerfully give away—in videos, in web pages, and in online discussion forums—the expert fruits of their labor, just to help one another.

None of these things were, exactly, predicted in advance. The founders of the Internet understood that they were producing a tool for human collaboration, and people who make tools inevitably make tools to make other tools. We are the inheritors of that beautiful, human tradition. Some of the very best of humanity is available online, every day, and we should not forget that.

Now, I do not pretend that the Internet—or platforms that operate within it—enable only humanitarian efforts. In that way, the Internet is no different from previous communication technologies. Written letters could be used to promote sedition. The printing press spread falsehoods as well as truth. Telegraph, radio, and television have all been used to hurt as well as help. What the Internet brings is its interactive nature: the ability of anyone to talk to anyone or even everyone, and the ability of everybody else to respond. That brings, unquestionably, dangers, but it also brings the sort of debate, uncontrolled by any gatekeeper, that the Founders of the United States of America valued and promoted. Intermediaries on the network of all kinds are implicated in ensuring that kind of conversation can happen. Hasty or broad changes to Section 230, therefore, could be extremely bad for American society.

As noted above in response to question 1, Section 230 seeks to ensure that the person most directly responsible for a violation of law or other harm is the one who should be held accountable for it. Most often that will be the creator or poster of the offending content. Sometimes, an online platform might directly violate a law (as suggested in the Roommates.com scenario mentioned in question 3a). But very seldom will the appropriate party to be held liable be an Internet Service Provider, or a CDN, or a web hosting company, or any of the many other intermediaries that are essential to making the Internet function. And because Section 230 protects the full range of Internet users and intermediaries—and not just online platforms—it is a very poor vehicle which with to address social problems at the "application layer."

As Congress continues its focus on addressing significant social concerns in the online environment, it will be important to apply some analytic framework to any proposed regulation of the Internet. Any such framework must allow an understanding of what the proposal might do—not just in the cases where it is aimed, but also in the cases where it is not. The Internet Society has an Internet Impact Assessment Toolkit[6] that is intended to assist with those kinds of explorations, and we stand ready to help the Congress make those kinds of evaluations.

[6] https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/.