United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Communications and Technology

Responses to Questions for the Record

Mary Graw Leary

Professor of Law
The Catholic University of America, Columbus School of Law

Submitted May 13, 2024

1. If I want to see this from a risk-based approach, what criteria and reporting requirements would that encompass, such as to the Federal Trade Commission?

a. Could this lead to a "rating" system of sites that use certain algorithms, such as to protect children?
b. Should there be a warning label, parental permission, etc.?

This question frames the issue of §230 immunity as one of risk assessment. Policy creation and reform to address the complex issues presented by today's Internet in a post §230 *de facto* near absolute immunity world can seem to require the balancing of some risks. However, regarding issues of child abuse and exploitation,[1] there should be no acceptance of a risk for those as acceptable tradeoffs for some other perceived benefit. Indeed, the last nearly three decades of *de facto* near absolute immunity have demonstrated that the concept of "risk" has played an entirely different role in the development of harmful practices by platforms. Courts have incorrectly interpreted §230(c)(1) immunity as immunity for platforms from nearly all accountability for harms they cause. Consequently, they not only allow abuse and exploitation on their platforms, but they facilitate it and even design their products to knowingly produce significant harm.[2]

The question seems to suggest that some of the perceived benefits of §230 could be retained and a portion of the risks mitigated through legislation which might continue some form of immunity but create a reporting requirement, rating system, or labelling system. With regard to §230(c)(1), that is not the most effective approach. The problem is the current overbroad court interpretation of §230(c)(1) immunity, and that section of §230 should be legislatively eliminated. As such, platforms would function

[1] To be clear, this term includes all forms of abuse and exploitation not only against children. Furthermore, this point is also true for a host of victimizations including, but not limited to, online bullying, violence, stalking, threats, other forms of sexual exploitation, etc. These comments reference abuse and exploitation as that was the subject of my original testimony.

[2] For a thorough discussion of the moral hazard created by the current overly broad interpretation of §230(c)(1) see Written Testimony of Dr. Mary Anne Franks, U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Communications and Technology Hearing: "Where Are We Now: Section 230 of the Communications Decency Act of 1996" (April 11, 2024). *See also,* Statement of Frances Haugen, U.S. Senate Committee on Commerce, Science, and Transportation, Subcommittee on Consumer Protection, Product Safety, and Data Security (Oct. 1, 2021); Statement of Arturo Bejar, U.S. Senate Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law (Nov. 7, 2023).

like any other industry and must take certain steps that include minimizing or eliminating the risk of harm from their product – just like every other business must do. Big Tech has litigated throughout the nation that it has near absolute immunity and, in other words, should have an existence free of accountability – unlike any other industry -- and that it has no duty of care to its customers or consumers.[3]

Given that this is the current climate caused by §230(c)(1), retaining this form of immunity but implementing a rating system will not provide the level of accountability necessary to minimize the risk to children. Rather, another approach will more significantly minimize the risk to children and other people vulnerable to abuse and exploitation. That approach includes not only eliminating the *de facto* near absolute immunity of §230(c)(1), but also requiring platforms to incorporate safety by design and reporting requirements to a regulatory agency such as the Federal Trade Commission (FTC). Furthermore, requiring such platforms to have a duty of care to those who use their products, will also better advance the goal of minimizing risk to children and others.[4]

With regard to deploying protective tools to consumers, history teaches that the technology industry will promise such voluntary action but will not deliver it in a useful manner. In 1996 the industry promised such tools,[5] the legislation provided them immunity for the creation of such tools,[6] and

---

[3] Recently, this was the explicit litigation position of Tik Tok in a hearing regarding a motion to dismiss. Regarding tort and negligence liability, TikTok stated as follows:
"The Court: So you don't – you don't have a duty to –
Counsel [for TikTok]: Not as articulated.
The Court: -- to design a platform in a safe way. … That's what you want to argue.
Counsel: Well, what I'm arguing –
The Court: Yes or no? Yes or no?
Counsel: **Well, yes, I do want to argue that, Your Honor**."
In re Social Media Adolescent Addiction/ Personal Injury Product Liability Litigation, No. C 22-MD-3047 YGR (N.D Cal.), Hearing on Motion to Dismiss (Oct. 27, 2023) at 146-147 (emphasis added).

[4] The question is a bit unclear as to a rating system. If it is suggesting a regulatory agency require platforms to be rated, there may be some obstacles. Such systems are typically voluntary to avoid implicating government action and the First Amendment. *E.g.,* Entertainment Software Ass'n v. Blagojevich, 404 F.Supp. 2d 1051 (N.D. Ill. 2005).

[5] *E.g.,* Kara Swisher, *Ban On Online Smut Opposed*, Wash. Post, July 18, 1995, at D3. (describing how the tech industry lobbied Congress and promised technological tools to prevent explicit content).

[6] 47 U.S.C. §230(c)(2).

in the most recent Senate hearings Meta promised such tools would make a difference,[7] and yet NCMEC just released its latest CyberTipline statistics which continue to demonstrate the complete failure of these platforms to protect children. As discussed in my original testimony, the measurement of the massive growth of reports to the CyberTipline is a very quantifiable way to assess the harms on the Internet and the failure of platforms to address them. These statistics indicate a staggering failure to eliminate risk. The 2023 Report indicates that in the last year NCMEC received over **36.2 million** reports of suspected child sexual exploitation, a more than **12% increase** in reports just from the previous year. Of these, the number of files included in the reports also **increased by 19%** from the previous year to more than **100 million files.**[8] Not only are the numbers shocking, but the harm to children is becoming increasingly severe. In the last three years alone the number of reports that NCMEC labeled as" imminent threats" to children **increased by 130%.**[9] The platforms have created and facilitated a dangerous atmosphere for children and others, and failed to take sufficient steps to address the threats known to them and protect users, despite promises to the contrary. The CyberTipline numbers belie their promises and claims otherwise. The industry will never effectively address these issues because it monetizes this type of material and profits from it.[10] In short, the industry has demonstrated it cannot police itself and, as such, should be held to the accountability standards of every other business. Furthermore, because of the scope of their reach and the demonstrated abuse of their capabilities, they should be a regulated industry.[11]

---

[7] Testimony of Mark Zuckerburg, CEO Meta, Senate Committee on the Judiciary "Big Tech and the Online Child Sexual Exploitation Crisis," January 31, 2024 (noting Meta has "more to learn" but remains "ready to work with members of this committee, industry and parents to make the internet safer for everyone.").

[8] CyberTipline 2023 Report, available at https://www.missingkids.org/cybertiplinedata (last visited May 9, 2024).

[9] Id.

[10] *E.g.* Cathy McMorris Roger and Frank Pallone, Sunset of Section 230 Would Force Big Tech's Hand; The law has outlived its usefulness and made the internet a dangerous place for America's children, The Wall Street Journal (May 12, 2024) ("Big Tech is profiting from children, developing algorithms that push harmful content on to our kids' feeds and refusing to strengthen their platforms' protections against predators, drug dealers, sex traffickers, extortioners and cyberbullies. Children are paying the price, developing addictive and dangerous habits, often at the expense of their mental health."); Mary Graw Leary, Written Testimony U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Communications and Technology Hearing: "Where Are We Now: Section 230 of the Communications Decency Act of 1996" (April 11, 2024).

[11] *See*, *e.g.,* Danielle Keats Citron and Benjamin Wittes, The Internet Will Not Break: Denying Bad Samaritans §230 Immunity, 86 Fordham L. Rev. 401 (2017).

Parental permissions and warning labels may be important components of addressing online harms, in addition to the repeal of Section 230(c)(1) immunity. It is important to note, however, that the concept of safety by design in a more broad way is needed, as well as a clear duty of care to consumers which is enforceable. These are features of the Kids Online Safety Act (KOSA) which includes provisions that establish a duty of care including reasonable measures to mitigate risk of harm to children, conspicuously available safeguards for minors and their parents, privacy by default settings, and required third party audits and reports.[12] Additionally, requiring disclosure of algorithms and other transparency measures are also components of KOSA and will address some of the issues with algorithms.[13] These kinds of features, in addition to an end of *de facto* near absolute immunity will be the stronger risk minimizing framework.

2. Social media companies moderate content that can be biased in certain directions, while not showing consistent policies. And yet, there is more misinformation or AI algorithms that trend users toward more outlandish content that could lead to violent behavior. Past government approaches have included a "Fairness Doctrine" approach that has the FCC determining contrasting views were adequately provided for in chat conversations, messaging streams, etc., along with limits against gratuitous violence. How can we encourage more competition of alternative views that seek to inform and not misinform without going down the road of something like a revamped Fairness Doctrine approach? I ask partly over concerns in giving the FCC too much authority or leeway, pre-empting the market to work through issues, given current rules in the face of previous court decisions and committee action.

Section 230 was not designed to encourage alternative views per se. Rather, §230 emerged from a landscape of child protection and was designed in part to protect platforms from civil liability when they take steps to protect children and others from explicit content. These problems, which were the focus of my testimony and expertise, implicate criminal and tortuous activity, not speech. A clear distinction exists between speech and criminal or tortious acts and that should be the focus of legislative reform. Such reform involves a removal of §230(c)(1) immunity, a continuation of the protection for good Samaritan efforts to eliminate explicit material found in §230(c)(2), and the same liability all American businesses face for actions that lead to harm of others through violations of criminal or civil laws on the state and

[12] Kids Online Safety Act, S. 1409, 118th Cong. (2023); H.R. 7891, 118th Cong (2024).
[13] Id.

federal level. As the Committee knows, the Supreme Court is considering whether state governments can restrict editorial choices for platforms.[14] These platforms are not government entities but private companies. Therefore, they can and should monitor the content on their platforms to minimize victimization. But these entities cannot have it both ways. They have taken the position in litigation that they can control what is on their platforms, but then argue in motions to dismiss that they should continue to have *de facto* near absolute immunity when sued for abrogating that responsibility.

Some of the concerns in the question can be addressed through the aforementioned duty of care and liability for false information facilitated on their platforms. This is hardly unprecedented. Newspapers, bookstores, libraries, and other entities possess First Amendment protections, but they are not absolute. Said entities have publisher or distributor liability. In 1996 Congress was clear to preclude platforms from publisher liability. But the text and legislative history of §230 make clear that as entities that distribute material, distributor liability is appropriate.[15] That is to say that liability for material that the platforms know or should know is illegal will logically lead to more focus on addressing these problems. It is apparent that platforms have the ability to marshal a great deal of data about their users and the content trafficked on their platforms. Clearly returning §230 to its original intent of limited immunity for only good Samaritan activity will encourage companies to address more effectively false or misleading information on their platforms as they will be immune from suit for doing so, but exposed to risk for failing to act regarding known problematic material. With regard to information produced or expanded by their own algorithms, their liability may be even more comprehensive.

---

[14] Moody v. NetChoice, LLC., cert granted No. 22-277 (argued Feb. 26, 2024); NetChoice, LLC. v. Paxton, cert granted No. 22-555 (argued Feb. 26, 2024).

[15] *E.g.* Mary Graw Leary, Written Testimony U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Communications and Technology Hearing: "Where Are We Now: Section 230 of the Communications Decency Act of 1996" (April 11, 2024); Dr. Mary Anne Franks, Written Testimony U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Communications and Technology Hearing: "Where Are We Now: Section 230 of the Communications Decency Act of 1996" (April 11, 2024); Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC., 141 S. Ct. 13, 14 (2020)(Thomas, J.).

When discussing the role of these platforms and unrepresented viewpoints, more must be said about groups whose viewpoints have been silenced. Those include the viewpoints of victim survivors and state officials seeking to enforce state laws regarding online abuse and exploitation.[16] Both these groups have been silenced in their claims against platforms because the courthouse doors have been shut to them. They not only are deprived their day in court to prove their claims, but also the ability to gather support for these claims utilizing the process of discovery. Motions to dismiss are so vital to these companies because they prevent the public – including Congress – from learning the depth of the depravity of their business practices.[17] Secondly, states are unable to enforce their own criminal and public protection laws.[18] Such hand tying of law enforcement and silencing of victim survivors is a concern. These are the kinds of viewpoints that should have a right of access to the important public square: a court of law where they must prove their claims. Section 230's perverse interpretation allowing *de facto* near absolute immunity has effectively precluded this important civil right. This expansion of immunity for good Samaritan to all activities of bad actors must be corrected and §230 restored to its original purpose.

[16] *E.g.,* Mary Graw Leary, *The Indecency of the Communication Decency Act*, 41 Harv. J. L. Pub. Pol'y 553, 574-581 (2018).
[17] Mary Graw Leary, Written Testimony U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Communications and Technology Hearing: "Where Are We Now: Section 230 of the Communications Decency Act of 1996" (April 11, 2024).
[18] *Id.*