Questions For the Record

Mary Graw Leary,

Professor of Law, The Catholic University of America

Children's Safety in the Digital Era: Strengthening Protections and Addressing Legal Gaps

Senate Judiciary Committee

March, 2025

Introduction

Thank you for the additional question regarding character-based AI chatbot apps. While this technology is not a specific area of my expertise, it does illustrate some of the several problems of the toxic combination of (a) an unregulated tech industry, (b) that releases dangerous untested products harmful to children; and (c) that possesses near de facto absolute immunity for the harm it causes by doing so. Phrased another way, the release of AI chatbot apps without adequate safety measures in place is a product of this unregulated environment and an outdated § 230 of the Communicates Decency Act. That Act not only fails Congressional goals of incentivizing a safer internet, but encourages the opposite, which is especially dangerous with ever evolving technologies such as these. This situation further illustrates that Congress cannot meet 21st Century problems with a 20th Century tool. This QFR answer will address the harms being caused children through unregulated AI chatbot apps, the basic need for legislative action, the role of § 230 in this discussion, and potential steps to consider.

1. Children Suffer When Unsafe Products Are Unleashed on Them

First, there have been documented cases of how these products inflict harm on children. These character based chatbot apps are designed to replicate conversations with an actual person – using AI to adapt to the user and create their own content.[1] These chatbot apps are designed to appear enticing to young people, designed to encourage ongoing and continual use, and expose children to harmful content. Documented cases exist of such bots providing youth dangerous advice to engage in harmful behavior, sharing harmful content, and exposing children to sexualized imagery and conversation. Some examples include chatbots encouraging a child to kill his parents; encouraging a child to kill himself; providing dangerous guidance on topics including drug use, self-harm, eating disorders and sexual abuse; causing severe depression; and causing addictive dependence and isolation.[2] Because of their developing brains, children are at great risk of negative effects of such a product. Children are more vulnerable and less able to process the nuances of an artificial bot giving them this harmful information when designed to appear to be a human friend.[3]

---

[1] AI Chatbots and Companions – Risks to Children and Young People, https://www.esafety.gov.au/newsroom/blogs/ai-chatbots-and-companions-risks-to-children-and-young-people#:~:text=the%20United%20States.-,What%20are%20the%20risks%3F,to%20overuse%20and%20even%20dependency; Queenie Wong, *Teens Are Spilling Dark Thoughts to AI Chatbots. Who's To Blame When Something Goes Wrong?*, The Los Angeles Times (Feb 25, 2025); Bobby Allyn, Lawsuit: *A Chatbot Hinted a Kid Should Kill His Parents Over Screen Time Limits*, NPR (Dec. 10, 2024).

[2] AI Chatbots and Companions – Risks to Children and Young People, https://www.esafety.gov.au/newsroom/blogs/ai-chatbots-and-companions-risks-to-children-and-young-people#:~:text=the%20United%20States.What%20are%20the%20risks%3F,to%20overuse%20and%20even%20dependency.

[3] *See, e.g.*, Matthew Hastings, *What Do Parents Need to Know About AI Character Chatbots?*, Univ. of Col Newsroom (Dec. 2, 2024), https://news.cuanschutz.edu/news-stories/what-do-parents-need-to-know-about-ai-character-chatbots.

2. No Other Industry Can Release Such a Dangerous Inadequately Tested Product That Harms Children and Avoid Accountability for Doing So

This leads to the obvious question of how is it that an industry could put onto the market such a dangerous product without being confident that it is safe and, once it discovers the harm it causes, keep it on the market? The answer is found in two components of our technology ecosystem: the industry is entirely unregulated and the companies are not incentivized to make their products safe because of the current distorted interpretation of § 230 of the CDA.

Regarding regulation, I noted in my original testimony as well as the article entered into the record that there is a natural historical arc of regulation compellingly outlined by Professors Danielle Keats Citron and Benjamin Wittes in their 2017 article, *The Internet Won't Break.* They point out that historically burgeoning industries can begin without regulation. However, when these industries mature, the government recognizes they reached a stage where the industry can cause broad harm by a small error, and the government takes on its required role of public protector and provides minimal safety guardrails to fulfill that obligation.[4] Examples of this historical arc include public transportation, utilities, motor vehicles, water supply, chemical manufacturing, food supply, and agriculture. When these industries grew to where they could cause serious harm to large numbers of people, some form of outside oversight occurred.[5]

However, in the context of these digital platforms, the government has not intervened in that traditional way. The result is unprecedented harm as has been outlined in many congressional hearings.

This is where the role of §230 of the Communications Decency Act is particularly insidious. Although intended to be a shield for platforms' efforts to protect children, tech companies have distorted it to provide a near absolute de facto immunity for actions that harm children and other users. Consequently, in addition to having the luxury of an unprecedented unregulated climate, § 230 provides businesses an additional incentive to release unsafe products to the market: protection from any liability for doing so. Consequently, these companies and their surrogates not only vigorously oppose common sense regulation but also seek wider immunity.[6]

Although the scope and size of the tech industry alone compel regulation and Congressional action, the nature of the industry also compels greater Congressional oversight. The rapid expansion of AI is breathtaking, in just two years society has been transformed and there are currently hundreds of chatbot companion apps, millions of characters, and some

[4] Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 Fordham L. Rev. 401, 406 (2017)..

[5] *Id.*

[6] In 2024 tech companies continued to attempt to expand their already de facto near absolute immunity. Calise v. eta, 103 F.4th 732,742(9th Cir. 2024)("Meta invites us to reconsider the limitations we have previously recognized and encourages us to adopt a broader rule that would effectively bar 'all claims' 'stemming from their publication of information created by third parties.")

companies reaching a $1 billion valuation in that time.[7] While traditionally courts can provide some relief to those harmed by dangerous products, they are hampered in doing so when the product is part of the tech industry. The judicial system is both reactive and slow moving and not effective when the product is related to these technologies and is rapidly changing. Therefore, relying on courts to somehow mitigate these harms is particularly inappropriate in a rapidly changing sector. Legislation is necessary.

3. §230 Has Not Only Helped Create This Problem, It Amplifies It

The above section describes how § 230 of the CDA helps cause the problem of character chat bot apps – or other dangerous products – being unleashed on the public generally, and children in particular, by providing an incentive to do so with impunity. This section describes how § 230 then is being utilized to preclude access to justice by perverting it even more than has already occurred.

Textually, § 230 of the CDA *should* provide no protection for generative AI platforms, because the content is generated by the platform and § 230 of the CDA specifically protects platforms only when the content is from a third party. Specifically, § 230 of the CDA provides protection for "interactive computer services" (ICS) not "information content providers" (ICP).[8] An "information content provider" includes "any person or entity that is responsible, in whole *or in part*, for the *creation or development of information* provided through the Internet or any other interactive computer service."[9] By creating the character and generating the content of the communication between the user and character, the bot is creating the content. Furthermore, courts have recognized that ICS's can also be information content providers and lose protection.[10] Therefore, AI generated content should not be protected at all by § 230 because it is content generated in whole or in part by the platform which is then acting as an information content provider.

But Congress should take no comfort in such textual clarity, as the current state of the distorted § 230 of the CDA has been and will continue to be utilized by said platforms to argue they are not responsible for the harms their AI causes.[11] Indeed they have used the "material contribution" test to argue that although they assist in the content development, they are not content providers. Amazingly, the blame for the content then goes back on the user.[12]

---

[7] Queenie Wong, *Teens Are Spilling Dark Thoughts to AI Chatbots. Who's To Blame When Something Goes Wrong?*, The Los Angeles Times (Feb 25, 2025).

[8] 47 U.S.C. §230(c).

[9] 47 U.S.C. 230(f)(3).

[10] *E.g., Fair Hous. Council of San Fernando Valley v. Roommates.com*, LLC, 521 F.3d 1157, 1163 (9th Cir. 2008).

[11] Justice Thomas has noted the hypocrisy of the tech industry's claim of s230 protection for their own content. "In the platforms' world, they are fully responsible for their websites when it results in constitutional protections, but the moment that responsibility could lead to liability, they can disclaim any obligations and enjoy greater protections from suit than nearly any other industry." *Doe v. Snap, Inc*., 144 S. Ct. 2493, 2494 (2024) (Thomas, J., dissenting denial of certiorari) (mem.).

[12] *Compare, Fair Hous. Council of San Fernando Valley v. Roommates.com*, LLC, 521 F.3d 1157, 1163 (9th Cir. 2008) (finding the platform materially contributed to the illegality by providing a drop down menu of terms) with

Consequently, the textual clarity of § 230 is not helpful to the question of whether §230 should be updated to remove this protection. It absolutely should.

Many courts have articulated the need for § 230 of the CDA to reflect the current technological realities, not the outdated ones of the 1996 dial up internet era. Just last year, a Ninth Circuit judge warned of AI when noting that the application of §230 of the CDA to technologies unimagined in 1996

> stretch the statute's plain meaning beyond recognition. And they will continue to occur unless we consider a more limited interpretation of § 230(c)(1)'s scope of immunity. *In a world ever evolving and with artificial intelligence raising the specter of lawless and limitless protections under § 230(c)(1),* we should revisit our precedent and ensure we have grounded its application.[13]

Similarly, Justice Thomas articulated that states and the federal government must be free to update their laws "to make them more appropriate for an Internet-driven society."[14] This notion of a changing and more protective legal regime as technologies rapidly develop has been articulated by scholars[15] and even during the debate of the original CDA.[16]

4. <u>Potential Responses to the Emergence of AI Chatbots</u>

Therefore, the answer to these challenges is a more regulated internet and an end to §230's incentive to release harmful products with impunity. More specifically, there are two components to a Congressional response to the problem of AI chatbots in an unregulated industry with a current legislative regime of incentivizing harmful product release. The first is eliminating that incentive by reforming § 230. The second is implementing regulatory legislation that is responsive to AI and other technologies.

Regarding § 230, as my original testimony addresses, Congress should remove § 230(c)(1) of the CDA entirely. Providing any sort of protection to platforms for harmful products for children flies in the face of the original intent of § 230 of the CDA. If § 230(c)(1) of the CDA ever did serve a purpose, the internet is no longer a nascent industry in need of any protection. Rather, the people need protection from an unregulated industry which causes harm on them.

Within such a reform, Congress should also consider specifically including language in § 230 that AI generated content is not protected in any form by § 230 of the CDA.[17] This would preemptively address some of the claims in courts that AI is protected by § 230 of the CDA. In

---

O'Kroley v. Fastcase.Inc., 831 F.3d 352 (6th Cir. 2016)(finding search engine did not materially contribute to how information was displayed although it engaged in some form of editing information).

[13] *Calise v. Meta Platforms, Inc*., 103 F.4th 732, 747–48 (9th Cir. 2024) (Nelson, J., concurring)(emphasis added).

[14] *Malwarebytes, Inc. v. Enigma Software Grp*. USA, LLC, 141 S. Cut.13 (2020)(mem.).

[15] Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 Fordham L. Rev. 401, 406 (2017).

[16] 142 **Cong. Rec.** S686 (daily ed. Feb. 1, 1996) (statement of Sen. Pressler) ("I predict that this will be succeeded someday as we get into the wireless age by another act, maybe in 10 or 15 years. But this Telecommunications Act will provide us with a road map into the wireless age and into the next century.").

[17] *See, e.g.*, A Bill to Waive Immunity Under Section 230 of the Communications Decency Act of 1934 [sic] for Claims and Charges Related to Generative Artificial Intelligence, S. 1993, 118th cong. (2023-2024).

courts addressing this problem, a very fact specific inquiry occurs regarding how the particular AI product functions and distinctions between AI operations can be made which will cause great disparity and confusion among the courts.. In order to prevent splintered court decisions, Congress can act now to answer the question of whether AI chat bots are considered content creation with an emphatic yes.

Such a reform is essential because of the nature of the technology. Currently, if § 230 of the CDA protects a platform for harm caused by third party content, the argument goes that the victim can still seek liability from the content creator. However, with AI, there is no other individual content creator and a victim will literally be left without any recourse.[18] Such is not acceptable.

Reform of § 230 of the CDA is only a minimal step. It simply allows injured parties access to a courtroom to attempt to prove their case. Such a reactive approach, while providing some deterrence, does little to prevent the harm in the first place.

Secondly, the tech industry in general, and the AI chatbots in particular, should face guidelines exposing their hosts and developers to penalties if unsafe. As is expressed in recent legal claims against Character AI, a fundamental problem is the industry releasing untested or inadequately tested chatbots to the public which are deeply flawed and dangerous to consumers.[19] Beyond § 230 of the CDA, the products raise issues about product design having nothing to do with publication. Here, previously proposed legislation requiring such platforms to exercise the same duty of care as other industries, seems an essential component of safety. Elements of this approach are found in the Kids Online Safety Act and present a promising step to such platforms being held accountable for the release of dangerous products.[20] Safety by design must be embedded within the industry as well. That being said, a duty of care and requirement of safety by design should be accompanied by the repeal of at least §230(c)(1) protections. This portion of § 230 of the CDA has proven to incentivize the production of harmful products and serves no purpose.

Within these guidelines, Congress should include elements of transparency and auditing. It is essential that the technology behind the AI and algorithms be transparent. Furthermore, efforts of the platforms to test them prior to deployment should be an essential component of necessary acts prior to release. The results of these audits should be available for review.

Third, Congress should consider a regulatory body to oversee this industry. This body should remain under the control of Congress. Such an office could provide, *inter alia*, standards of care and best practices, which would give the industry a sense of acceptable safety standards.

As Congress considers the future of the internet and the valid concerns of the government's ability to stay in pace with rapidly changing technologies, there is an additional model to which some nations are turning due to the need for a rapid response to quickly developing threats. This

[18] See, Jake Gray and Abbey Block, *Beyond the Search Bar: Generative AI's Section 230 Tightrope*, Business Law Today (Nov.2024).
[19] *Garcia v. Character Techs, Inc*., No.6:24-CV-01903 (M.D. Fla. Oct. 22, 2024).
[20] Kids Online Safety Act, S. 1409, 118th Cong. (2023).

model is the creation of an E-Safety Commissioner. Australia was the first nation to do so. The purpose of the office is "to help safeguard [the public] at risk of online harms and to promote safer, more positive online experiences" and the Commissioner takes measures aimed at "preventing online risks, reducing the impacts of harms ,and building safer digital spaces."[21] Created in 2015, when Australia streamlined its online safety legislation in 2021 in the Online Safety Act, the Commission's mission included prevention, protection, and proactive system change.[22]

Essential to that effort was the 2021 Online Safety Act leading to a list of Basic Online Safety Expectations (BOSE) the government required of platforms.[23] These provisions, enforceable with significant civil penalties, outline Congress's expectations that social media, platforms, and other providers in the tech industry, will take reasonable steps to incorporate safety by design for all users.

By creating such **Congressional** expectations and then establishing an E-Safety Commissioner, Congress could embark on a more proactive regime necessary for the today's evolving digital world. Such an office likely would more nimbly address emerging threats online than Congressional action could do. If its powers were drafted narrowly enough to respond to such threats with Congressional oversight, this office may prove to be a valuable tool to enhance online safety.

To be clear, reform of § 230 and the creation of a clear duty of care should not wait for the establishment of this office. The harms people are experiencing are immediate and significant; and Internet regulation and § 230 of the CDA reform are long overdue. That being said, Congress should think more systematically about how the federal government can be positioned to respond to future threats and not wait for the threats to emerge. Therefore, an E-Safety Commission is worth further consideration.

Conclusion

AI Chatbots pose a serious threat to users, especially youth. No other industry could release a dangerous product to children with impunity. Court response to this will be slow and likely distorted. Therefore, Congress must act and do so in a way that is proactive and systemic. This has at least two major components to combat the uniquely toxic ecosystem that has been created by the distortion of § 230 of the CDA and a lack of meaningful regulation for such a powerful industry. At a minimum the §230of the CDA reforms should include the removal of § 230(c)(1) protection, and an explicit statement that those who develop, finance, host and power AI technologies are responsible for the harm their products create. Finally, meaningful regulation which lays out Congressional expectations of the tech industry and penalties for failure to conform are essential and the possible creation of an e-safety commissioner with Congressional oversight has promise to execute these visions.

[21] https://www.esafety.gov.au/about-us/what-we-do
[22] https://www.esafety.gov.au/about-us/what-we-do
[23] Online Basic Online Safety Expectations - Determinations 2022, https://www.legislation.gov.au/F2022L00062/latest/downloads