The World Wild Web: Examining Harms Online

ETHICS AND PUBLIC POLICY CENTER
Shaping Policy, Renewing Culture.

March 26, 2025

Written Testimony of Clare Morell, Fellow, Ethics and Public Policy Center
Before the U.S. House Subcommittee on Commerce, Manufacturing, and Trade

Summary

- Screen time limits are no match for digital technology's underlying addictive design that is harming the development, relationships, and health of America's children
- Parental controls are extremely limited in the protection and oversight they can provide to parents to keep children safe from predators and dangerous content online
- Content filters are ineffective in protecting children from online pornography in the smartphone, social-media era of the internet
- The collective nature of the harms from digital technologies make it extremely difficult for individual parents to successfully protect their children or even opt out of them entirely
- There has been no legal accountability for digital technology companies' harms to children, America's youngest consumers
- Parents need legislation from the government to help them effectively protect their children from online dangers

Good morning, Chairman Bilirakis, Ranking Member Schakowsky, and distinguished members of the Committee.

My name is Clare Morell and I am a fellow at the Ethics and Public Policy Center (EPPC), where I direct EPPC's Technology and Human Flourishing Project. The focus of our project is exploring how technology can both advance and undermine human dignity and human flourishing.[1] We put out resources for policymakers on solutions to protect kids online, like reports and model legislation on age-verification for pornography websites and parental consent for social media. These laws have now been implemented in several states, 19 states have passed age-verification for pornography websites and nine states have passed parental consent for social media. Protecting kids online is a bipartisan goal and I have been grateful to see both point red and blue states adopt laws to protect kids online.

[1] https://eppc.org/program/technology-and-human-flourishing/

I am also the author of the forthcoming book, *The Tech Exit: A Practical Guide to Freeing Kids and Teens from Smartphones*, which will be published by Penguin Random House on June 3 of this year. The book offers a practical roadmap for parents of how to delay smartphones and social media for their children and live out a screen-minimal lifestyle as a family, as well as what schools and policymakers can do to support parents in protecting kids from digital harms.[2]

My experience researching and conducting interviews in the process of writing this book, along with my public policy work over the last several years, has firmly convinced me that America's parents need better laws to help them in protecting their children online. Screen time limits and parental controls are not working for parents or children. Children are not effectively protected from the harms of digital technologies and parents are frustrated and exasperated doing everything they can to stay on top of all the different apps, controls, settings, and thousands of portals of entry to the online world, with countless loopholes and workarounds to try to close down. Individual parents are up against enormous technology companies, with unlimited resources, employing predatory business practices towards children and operating with near complete impunity due to the lack of legal accountability in the internet industry, and the tools available to parents are extremely limited and unable to give them effective oversight over children's online experiences. Nor do current tools address the root issues behind the harms to children, like the addictive product design and the collective group harms created by these technologies. It is nowhere close to a fair fight.

I want to therefore focus my testimony today on explaining for the committee why this is the case – why the harms to children today from the worldwide web are no match for the current tools and strategies parents have available. I will conclude my testimony by offering a few categories of solutions for Congress to consider that would make a significant impact in protecting America's children from digital harms and empowering parents over their children's online behavior.

Screen Time Limits are No Match for the Addictive Design of Digital Tech

Screen time limits are the most common recommendation pushed on parents to curtail kids' use of social media. But the reality is that they are wholly insufficient. In even a short amount of time on an app or device a child can be exposed to harmful material or dangerous strangers.

Time limits also do nothing to address the inherent addictive nature of these technologies. Even if a child is only on social media for 15 minutes a day, the craving it creates means they are mentally consumed by what's happening on the app even when they aren't actively using it. And it means the limit is never enough, resulting in a hundred screen time battles a day between child and parent.

This is because smartphones and social media apps are designed to undermine any impulse control or effort to use them in moderation. Online companies are actively recruiting, targeting, and profiting off of minors, all while knowing their products are harmful to children, their brains, mental health, and development. These are predatory businesses. These companies completely ignore COPPA and actively recruit underage users, as recent lawsuits by states' attorneys general have revealed.

2 https://sites.prh.com/thetechexitbook

Social media companies are financially motivated to attract and retain *young* users. As one Meta product designer summarized in an internal email, "[s]hort summary is the 'the [sic] young ones are the best ones.' You want to bring people to your service young and early."[3] This is despite knowing their products are addictive and harmful to kids. Meta executives were informed in internal reports that teens regularly reported wanting to spend less time on Instagram, but "they often feel 'addicted' and "feel unable to stop themselves."[4] Meta is not alone. Internal TikTok documents, only recently made public through litigation by states' attorneys general, also document that the company is well aware that "minors do not have executive function to control their screen time," that minors are "particularly sensitive to reinforcement in the form of social award" and have "minimal ability to self-regulate effectively," and that its algorithms take advantage of this developmental incapacity in order to keep young users on the app for as many hours of the day as possible. When TikTok designers proposed modifications to reduce addictive use of TikTok, senior management was only willing to consider changes that would result in no more than a 5% drop in "stay time."[5]

Developing brains are especially vulnerable to the addictive aspects of social media. The regions of the brain associated with social rewards, like visibility, attention, and approval from peers, undergo significant development during adolescence. The brain's dopamine receptors multiply between the ages of ten and twelve. In contrast, the prefrontal cortex, which enables self-control, isn't fully developed until age twenty-five.[6] As Professor Mitch Prinstein has explained, "[d]ata reveal that social media stimuli, such as receiving 'likes' or followers activates the social reward regions of the brain. In other words, these features of social media capitalize on youths' biologically based need for social rewards before they are able to regulate themselves from over-use."[7] In simpler terms, children's brains are "all gas pedal with no brakes" when it comes to craving the social feedback that tech readily and constantly serves up to kids.[8]

And a brain exposed frequently to social media closely resembles a brain hooked on the most highly addictive drugs.[9] Time limits cannot sufficiently mitigate these addictive effects. Even if children are allowed on social media for only thirty minutes a day, that brief exposure can affect their mental space for the rest of the day. Social media is designed to make people check their accounts compulsively. Because of the built-in social metrics, children will be constantly thinking about the next time they can get on to see what likes they may have gotten or what friends might be posting. Parents I've spoken with share that even 15 minutes a day was enough to create a compulsive craving for an app. Their child would spend the rest of the day thinking about the app and when they could get back on it. It mentally consumed them. This underlying addictive design means that whether a child spends fifteen minutes or an hour in the virtual world, they will carry it with them mentally and emotionally long after they visually leave the apps.

3 *State of Arizona et al. v. Meta Platforms et al.*, No. 4:23-CV-05448 (N.D. Calif. 2023), oag.ca.gov/system/files/attachments/press-docs/Less-redacted%20complaint%20-%20released.pdf; "Attorney General Bonta: Unredacted Federal Lawsuit Against Meta 'Damning,' " Office of the Attorney General, State of California Department of Justice, November 27, 2023,oag.ca.gov/news/press-releases/attorney-general-bonta-unredacted-federal-lawsuit-against-meta-%E2%80%9Cdamning%E2%80%9D.

4 Georgia Wells, Jeff Horwitz, Deepa Seetharaman, "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show," *The Wall Street Journal*, September 14, 2021, https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739

5 *Commonwealth of Kentucky v. TikTok* Complaint, Filed October, 8, 2024, https://www.iccl.ie/wp-content/uploads/2024/12/TikTok-Kentucky.pdf

6 Zara Abrams, "Why Young Brains Are Especially Vulnerable to Social Media," American Psychological Association, last modified August 3, 2023, apa.org/news/apa/2022/social-media-children-teens.

7 Mitch Prinstein, Protecting Our Children Online (Washington, D.C.: U.S. Senate Committee on Judiciary, February 14, 2023) judiciary.senate.gov/imo/media/doc/2023-02-14%20-%20Testimony%20-%20Prinstein.pdf

8 *Ibid.*

9 Lin, Fuchun & Lei, Hao. (2017). Structural Brain Imaging and Internet Addiction. 10.1007/978-3-319-46276-9_3.

The negative effects from digital technology's dopamine-inducing features also do not only occur when someone is spending too much time on them. But even regular use has been found to be detrimental to developing brains. A University of North Carolina study in 2023 found that sixth and seventh grade students who checked social media platforms (Facebook, Instagram, and Snapchat) multiple times throughout the day, not considering the amount of time spent, demonstrated divergent brain development over time. Students who were frequent checkers of social media became more sensitive over time to social feedback compared with students who didn't check social media as often.[10]

The Myth of Parental Controls

It's not only the inherent addictive design of digital technologies that makes them dangerous. They are also a threat to children because the online world is rife with predators and dangerous content. Most parents are aware of these threats and are told to turn to parental controls for protection, but the question is whether these measures are working out. From my research the answer is an unequivocal no, the controls are not working for parents.

Social media companies have worked to convince parents that if they just enable the parental controls on their apps, their children will be safe. Instagram, along with many of the other major social media platforms like Snapchat, TikTok, and Discord, offers "parental supervision" tools, but in all cases, with the narrow exception of certain new defaults for Instagram accounts for 13- to 15-year-olds that require parental approval to change, the teen always has to accept the parent's supervision and can cancel it at any time (though the parent will get a notification if it's canceled).[11]

And even that supervision is extremely limited. The parental "controls" that platforms and apps offer really only allow parents to set daily time limits and breaks, manage privacy settings and content restrictions, see the child's following and followers lists (or in the case of Instagram and Snapchat, who they are messaging), and view any reports the child submits. But the parent has no insight into posts in the child's feed or the content of messages sent and received. Parents can't meaningfully oversee children's online activity, nor can account restrictions truly be locked in by a parent, meaning the idea that these are parental controls, in any sense of that word, is a myth. Content restrictions in apps are also often ineffective. One mom who had activated TikTok's Restricted Mode found during her test run that all the videos in the feed were still inappropriate for her child, including one video that was a play on ejaculation.[12] App settings are thus more like suggestions.

Even more frustrating, external parental control apps and filters that parents can purchase don't have access to the content and messages *inside* of the apps. External parental control software can help parents monitor or block dangerous material. For example, Bark monitors a child's texts, emails, web browser activity, and some apps using its AI technology and sends the parent alerts if it detects explicit images or

10 Maria T. Maza et al., "Association of Habitual Checking Behaviors on Social Media with Longitudinal Functional Brain Development," JAMA Pediatrics 177, no. 2 (2023): 160–67, doi.org/10.1001/jamapediatrics.2022.4924.

11 "About Instagram Teen Privacy and Safety Settings," Help Center, Instagram, help.instagram.com/3237561506542117; "About Instagram Teen Accounts," Help Center, Instagram, help.instagram.com/995996839195964?helpref=faq_content; "Guardian's Guide," Safety Center, TikTok, tiktok.com/safety/en/guardians-guide; "Tools and Resources for Parents," Parents, Snapchat, parents.snapchat.com/parental-controls? lang=en-US.

12 TikTok App Review, Protect Young Eyes, protectyoungeyes.com/apps/tiktok-parental-controls/.

other unsafe content, like cyberbullying, violence, or drug/alcohol content.[13] Another software called Canopy also uses AI to detect nudity in web browsers or photos taken on or downloaded to a device, blocks out explicit content in real time, and prevents a child from accessing or sharing a potentially risky photo until it's reviewed by the parent.[14]But some of the most common apps where illicit photos and other dangerous content are shared or viewed, like Snapchat, TikTok, and Discord, all block access to third-party controls, or in the case of Instagram, block their access to direct messages.[15] Parents are flying blind when it comes to social media.

Controls also can't filter out the environment that these apps create, where teens are incentivized to post sexualized content of themselves or participate in illicit sexual activities. A Forbes review of hundreds of TikTok livestreams revealed "how viewers regularly use the comments to urge young girls to perform acts that appear to toe the line of child pornography—rewarding those who oblige with TikTok gifts, which can be redeemed for money, or off-platform payments to Venmo, Pay-Pal or Cash App accounts. It's 'the digital equivalent of going down the street to a strip club filled with 15-year- olds,' says Leah Plunkett, an assistant dean at Harvard Law School."[16]

Devices make it worse, not easier, for parents. Although Apple and Google both advertise parental control settings to parents, they don't make them easy or intuitive to turn on. For example, Apple's Screen Time is a horrible name for its parental controls because it doesn't even indicate that this feature includes an adult website filter and other content restrictions a parent can turn on. One guide developed by Protect Young Eyes, a leading parental advising organization, outlines the *seventeen* different steps required to set up Screen Time on an iPhone or iPad.[17] Even if a parent does navigate their way to activating device controls, they are buggy and often don't work effectively. And device content restrictions, like restricting available apps in the app store to only be for a certain age range, like 9+ or 12+, the app ratings are often deceptive.

A recent article in *the Wall Street Journal* highlights how researchers over a 24-hour period in the Apple App Store found about 200 apps with inappropriate content that were rated as safe for children. "Those included apps for dieting, circumventing banned sites, beauty filters, violent or sexual games, and anonymous chat, according to a report by the child safety advocacy nonprofits Heat Initiative and ParentsTogether Action…The findings suggest that many apps including objectionable content for children are rated as safe."[18] The article gives several examples, like "apps that facilitate chats with strangers are widely available for ages 12 and above, including Spin the Bottle: maybe you?, which advertises to users: 'Sit at any table to meet new people, flirt and chat.'"[19] Parents also say advertisements promoting sexual content and adult apps are showing up inside apps intended for children.[20] It doesn't matter then whether a parent uses the device's parental control settings to restrict available apps to a

13 Home page, Bark, bark.us.

14 Home page, Canopy, canopy.us.

15 Some companies, like Bark, have found workarounds on Androids to access app data from the device itself, but this is not possible on Apple's closed system, which means since the majority of teens have iPhones, third party monitoring software has no access to their social media activity on apps like Snapchat that block access. Bark, What Bark Monitors, https://www.bark.us/what-bark-monitors/ (comparing iOS and Android devices).

16 Alexandra S. Levine, "How TikTok Live Became 'a Strip Club Filled with 15-Year-Olds,'" Forbes, April 27, 2022, forbes.com/sites/alexandralevine/2022/04/27/how-tiktok-live-became-a-strip-club-filled-with-15-year-olds/?sh=2688e23062d7.

17 Protect Young Eyes, Apple (iOS) Parental Controls, https://protectyoungeyes.com/devices/apple-ios-iphone-ipadparental-controls/

18 Aaron Tilley, "Apple's App Store Puts Kids a Click Away From a Slew of Inappropriate Apps," *The Wall Street Journal*, December 22, 2024, https://www.wsj.com/tech/apples-app-store-puts-kids-a-click-away-from-a-slew-of-inappropriate-apps-dfde01d5

19 *Ibid.*

20 Brian Pia, "Sexually Suggestive Ads Appearing on Children's Apps," ABC 33/40 News, December 2, 2017, abc3340.com/archive/sexually-suggestive-ads-appearing-on-childrens-apps

certain age rating if the age ratings are not accurate or inappropriate ads can be shown in any app.

Given the ineffectiveness of controls, a parent may rightly decide to keep their child off of social media entirely—which I personally encourage parents to do in my forthcoming book, *The Tech Exit*—but even then, parents still aren't completely in the driver's seat. Determined kids can too easily go behind their parents back to create accounts. All they have to do is enter a false birth date, check a box, and they're on. There is no age verification or parental involvement required in the creation of a social media account whatsoever.

The Ineffectiveness of Content Filters

Social media and smartphones have also ushered in a wave of online pornography exposure and subsequent addiction among America's youth. Pornography, especially the violent and dehumanizing kinds that are common today, has profound effects on children's mental and physical health. A survey by Common Sense Media found that most teens who have viewed pornography "have been exposed to aggressive and/or violent forms of pornography. This includes 52% who reported having seen pornography depicting what appears to be rape, choking, or someone in pain."[21] And children are not just seeing it, but acting it out. Nurses report a growing trend of children sexually abusing other children.[22] Recent studies have also found that pornography is powerfully addictive, analogous to addictive behaviors (gambling) and substances (tobacco, alcohol).[23]

Unfortunately, as I recently explained in an amicus brief submitted to the Supreme Court in the case *Free Speech Coalition v. Paxton* over the constitutionality of Texas's age-verification law for pornography websites, content filters employed by parents have not been effective in shielding children from online pornography.[24] Content filters are supposed to help parents protect their children by blocking access to pornography. However, they have significant loopholes, are prone to glitches and bugs, and often don't work inside of apps and in-app browsers.

Content filters operate on internet browsers, which on desktops and laptop computers serve as the means of accessing the internet. But for smartphones, the internet is often accessed via apps that possess their own in-app browsers, which are generally outside the purview of content filters.[25] This makes it easy for minors to access porn on their phones, even if their parents have protected the phone's browser, like Safari or Google Chrome, with a filter.[26] Consider Snapchat, a popular social media platform whose app is rated 12+ on Apple's App Store. A minor with the Snapchat app on his phone

21 Robb, M.B., & Mann, S. (2023). Teens and pornography. San Francisco, CA: Common Sense

22 The Influence of Pornography on Child Sexual Assault, Culture Reframed, July 27, 2023, https://culturereframed.org/theinfluence-of-pornography-on-child-sexual-assault/.

23 Your Brain on Porn, Brain Studies on Porn Users & SexAddicts, https://www.yourbrainonporn.com/relevant-researchand-articles-about-the-studies/brain-studies-on-porn-users-sexaddicts/#brain. (collecting findings from more than 35 neurological studies)

24 Brief for Clare Morell and Brad Littlejohn as Amici Curiae, No. 23-1122, Supreme Court of the United States, *Free Speech Coalition Inc. v. Paxton*, November 22, 2024, https://eppc.org/wp-content/uploads/2024/11/20241122181620210EPPC-Scholars-Brief-Free-Speech-Coalition-FILED.pdf

25 Canopy cannot filter content within non-browser apps. Canopy, Internet Safety FAQs, https://canopy.us/internet-safety-faq/; Covenant Eyes has said they are not permitted to filter in other third-party browsers, including hidden in-app browsers, though some users have had mixed results on this; Covenant Eyes, Hidden browsers in apps, Covenant Eyes Serv. Ctr., https://support.covenanteyes.com/hc/enus/community/posts/1501 9233976987-Hidden-browsers-in-apps;

26 Jake Cutler, What are Embedded Web Browsers? A Guide for Parents, Gabb Now, Nov. 1, 2023, https://gabb.com/blog/embedded-web-browsers/.

can get to PornHub in just five clicks.[27] Third-party filters would be of no help because Snapchat—like TikTok and Discord—blocks them.[28]

Kids don't even need to go looking for porn on the web—it finds them on social media. In one leaked study, nearly a fifth of teens ages thirteen to fifteen saw sexually explicit content at least once a week on Instagram.[29] Filters that can block adult websites or nudity in a web browser are powerless to filter out the explicit content being distributed within the apps themselves.

Parents have also discovered that the restrictions they have set on their children's smartphones often don't stick or have serious bugs. Content filters can even deactivate entirely after a software update.[30] Or have serious loopholes, as a Wall Street Journal reporter who tested Apple's controls wrote: "My son's iPad is set to restrict him from visiting most websites. And yet I was able to use it to access the most X-rated parts of the internet. Porn, violent images, illicit drugs. I could see it all by typing a special string of characters into the Safari browser's address bar. The parental controls I had set via Apple's Screen Time? Useless."[31]

The ease of accessibility to internet pornography in the smartphone and social media era, combined with the ineffectiveness of app content restrictions and filters' loopholes and inability to filter out the explicit content inside apps' feeds, means parents in practice are unable to proactively protect their children from pornography's harms. And so, children are being exposed to porn young and often. In a 2022 study, 73% of the teens surveyed reported that they had been exposed to porn. The average age of first exposure was twelve. More than half had encountered it accidentally. Of those, 63% said they had been exposed in the past week, suggesting it's a frequent experience. Much of the accidental exposure came from online means.[32]

Children's pornography exposure is also a justice issue. The current status quo leaves children of lower-income families especially vulnerable. First, such children have, on average, almost twice as much screen time as their higher-income peers.[33] Second, lower-income households are less likely to monitor their children's devices. A non-profit focused on protecting children from commercial sexual exploitation testified in a Texas state hearing that they have seen "a strong correlation between wealth and privilege and using filtering technologies. That is, well-heeled parents generally have the time and resources to use filters while low-income parents do not."[34]

27 Chris McKenna, Warning: Pornhub is on Snapchat. And Parents Have No Idea, Protect Young Eyes, June 30, 2019, https://protectyoungeyes.com/warning-pornhub-is-on-snapchatand-parents-have-no-idea/.

28 See note 15 *supra*.

29 *State of New Mexico v. Meta Platforms et al.*, No. 1:23-CV-01115-MIS-KK(D.N.Mex. Jan. 19, 2024), Document 36-2, storage.courtlistener.com/recap/gov.uscourtsnmd.496039/gov.uscourtsnmd.496039.36.2.pdf.

30 Apple Community (NeilKY), iOS Updates disable Parental Controls/Downtime on Kids phone (iOS 16+) (Feb. 17, 2024, 6:07 AM), https://discussions.apple.com/thread/254647836?sortBy=rank; Apple Community (sarwag13), parental controls keep resetting after 16 update (Jan. 16, 2023, 1:55 PM), https://discussions.apple.com/thread/254561788?sortBy=rank.

31 Joanna Stern, "How Broken Are Apple's Parental Controls? It Took 3 Years to Fix an X-Rated Loophole," *The Wall Street Journal*, June 5, 2024, www.wsj.com/tech/personal-tech/a-bug-allowed-kids-tovisit-x-rated-sites-apple-took-three-years-to-fix-it-17e5f65d

32 Robb, M.B., & Mann, S. (2023). Teens and pornography. San Francisco, CA: Common Sense.

33 Victoria Rideout et al., "The Common Sense Census: Media Use by Tweens and Teens," (San Francisco: Common Sense Media, 2022), commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf. (Kids in homes with annual income less than $35,000 spend on average 7:32 hours each a day on screens; kids in homes with annual income over $100,000 spend on average 4:21 hours a day on screens).

34 Testimony of Jamie Carruthers on S.B. 417, Tex. Sen. Comm. State Affs., at 2:18:20 (Apr. 3, 2023), https://senate.texas.gov/videoplayer.php?vid=19131&lang=en.

Individual Parents Cannot Address the Collective Harms

The teen mental health crisis today is due not only to negative effects of digital technologies for individuals but also to the group social dynamics that smartphones and social media have created. Dr. Jonathan Haidt in his book, *The Anxious Generation*, explains that smartphones with their social media apps harm all teens' social lives. These technologies create negative network effects where, even if a few tweens or teens use them in a school or organization, it affects the entire cohort of young people, including those who don't use social media apps at all.[35]

Time limits can make no impact on a child's social environment and the nature of children's friendships. Since teen relationships are now largely mediated through what's happening in the online world of social media, individual families imposing screen-time limits are not able to address this dynamic. Thus, while studies show that reducing the time spent on social media does reduce mental health symptoms, limits on time can't eliminate the negative social dynamics from screens, which also undermine real friendship, induce loneliness and anxiety, and can lead to depression, even for teens not on the apps.[36]

The risks of tweens and teens' social media use are not isolated to the individual users, but can make the environment unsafe for everyone, both from dangerous content shared by one child with another, and through the negative social environment created even for teens not on the apps. Even if parents could effectively control and filter their children's devices, they still couldn't protect their children from seeing porn on another child's device. In this smartphone era, any other kid on the bus or school can too easily lean over and put pornography in front of them. In fact, a study by the Oxford Internet Institute estimated that a caregiver's use of filters only reduced by 0.5% — one in 200 — the chance that a child would encounter online sexual material.[37] Putting the burden on parents alone to solely rely on their own controls and filters is not enough, and simply means that the lowest common denominator will prevail, with the least-regulated households setting the tone for the children's community as a whole.[38]

Parents cannot sufficiently protect their children from digital harms alone. Children's social media and smartphone use and pornography exposure are collective action problems. Parents need better laws to back them up.

35 Jonathan Haidt, *The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness* (New York: Penguin, 2024), 148–50; see also Jonathan Haidt, "Social Media Is a Major Cause of the Mental Illness Epidemic in Teen Girls. Here's the Evidence," After Babel, Substack, February 22, 2023, afterbabel.com/p/social-media-mental-illness-epidemic.

36 Melissa G. Hunt et al., "No More FOMO: Limiting Social Media Decreases Loneliness and Depression," Journal of Social and Clinical Psychology 37, no. 10 (2018), guilfordjournals.com/doi/10.1521/jscp.2018.37.10.751

37 Andrew K. Przybylski & Victoria Nash, Internet Filtering and Adolescent Exposure to Online Sexual Material, 21 Cyberpsych. Behav. Soc. Networking 405 (2018), https://www.ncbinlm.nih.gov/pmc/articles/PMC6101267/.

38 Brief for Clare Morell and Brad Littlejohn as Amici Curiae, No. 23-1122, Supreme Court of the United States, *Free Speech Coalition Inc. v. Paxton*, November 22, 2024, https://eppc.org/wp-content/uploads/2024/11/20241122181620210EPPC-Scholars-Brief-Free-Speech-Coalition-FILED.pdf

Current Legal Challenges

Tech companies have been able to get away with harms to children because they have faced little to no legal accountability for their harms, hiding behind the immunity shield of Section 230 and its overexpansion by courts. As Justice Clarence Thomas has explained, Section 230 was designed to give internet companies immunity from publisher liability for content they host, not to also give them immunity from distributor liability, shielding them from legal penalties for distributing illegal content like obscenity or drug trafficking, nor to give them immunity for wrongdoing related to their own product design, like algorithms recommending child victims to human traffickers and sexual predators.[39]

To give one tragic example, Ten-year-old Nylah Anderson was found by her mother unconscious, hanging from a purse strap, in her bedroom closet after performing a TikTok blackout challenge. She was rushed to the hospital but died five days later. Her mother, Taiwanna Anderson, filed a wrongful-death lawsuit against TikTok for the app's role in recommending the deadly challenge on her daughter's For You feed. The federal judge on the case, however, dismissed the lawsuit, citing Section 230.[40] But little Nylah Anderson would likely have never come across such a horrifying and dangerous challenge had TikTok not fed it up to her. Yet hiding behind the massive shield of Section 230, platforms have been able to avoid accountability for such harms. No litigation, no accountability, means no incentives for companies to change their behavior. Children's deaths will be business as usual unless the law changes.

Section 230 has thus caused a growing disparity between the real world and the online world. The normal legal means of holding companies accountable, litigation and consumer protection, have been largely closed off for all internet companies.

In hopeful news, some courts are stepping up to help clarify and restore Section 230's interpretation to the original meaning of the law. The Third Circuit recently revived Ms. Anderson's lawsuit, sending it back to the district court for trial. In his concurrence to the decision, Judge Paul Matey wrote that Section 230 does not shield TikTok for its "knowing distribution and targeted recommendation of videos it knew could be harmful."[41]

The First Amendment has also been a challenge. Any attempt to age-restrict portions of the internet or require parental consent for social media are met with cries from tech companies that it violates the First Amendment and the free speech rights of adults and minor's rights to speech. But we must recognize that the technology has changed vastly from 2004 when the Supreme Court last considered an age-verification law in the *Ashcroft v. ACLU* case and ruled that filters, employed by parents, was "an effective and less restrictive means." Twenty years later with vast technological changes, filters are not remotely effective in shielding kids from porn in the smartphone, social-media era of the internet, while on the other hand, positive technological changes now mean there are many age verification methods available online that are anonymous and convenient for adults, and impose little to no burden on adult speech. With the development of techniques relying on zero-knowledge proofs, now widely used in cryptocurrency, other cryptographic techniques, and digital IDs, anonymous online authentication of age is possible. Age verification can in fact be the least restrictive means for adults and the best means to effectively protect children.

39 Statement of Clarence Thomas, *Malwarebytes v. Enigma Software,* 592 U.S. 1 (2020), supremecourt.gov/opinions/20pdf/19-1284_869d.pdf.

40 Angela Yang, "Judge Dismisses Suit Alleging TikTok 'Blackout Challenge' Caused Girl's Death," NBC News, October 26, 2022, nbcnews.com/news/judge-dismisses-suit-alleging-tiktok-blackout-challenge-caused-girls-d-rcna54208.

41 *TikTok v. Anderson*, United States Court of Appeal for the Third Circuit, No. 22-3061, Judge Paul Matey, Concurring Opinion, August 27, 2024, https://www2.ca3.uscourts.gov/opinarch/223061p.pdf

Furthermore, the free speech rights of minors are questionable and limited and do not supersede parents' rights to raise their children, a precedent recognized for a century in cases such as *Pierce v. Society of Sisters*. In fact, Justice Clarence Thomas has written that "the 'freedom of speech,' as originally understood, does not include a right to speak to minors (or a right of minors to access speech) without going through the minors' parents or guardians." There is certainly no First Amendment right for companies to contract with children in order to speak to them over their parents' objections, but this is precisely what social media companies do, since there is no parental involvement whatsoever in minors entering into online contracts with social media companies.

Our Founders intended the First Amendment to be a bulwark to protect our speech, not to be used as a sword for Big Tech and the porn industry to cut down any measure to protect children from their harmful products. As Third Circuit Judge Matey recently lamented in his concurrence in *TikTok v. Anderson*, this perspective is shared by "a host of purveyors of pornography, self-mutilation, and exploitation…[to] smuggle constitutional conceptions of a 'free trade in ideas' into a digital 'cauldron of illicit loves' that leap and boil with no oversight, no accountability, no remedy."[42]

In summary, we should not have one constitutional regime that governs the real, physical world and a different constitutional regime that governs the online world. The goal should be to make those regimes as equal as possible. To do so we need critical changes in the law.

The Laws Parents Need

1. Restrict Social Media out of Childhood

Given the compelling evidence, Congress should age-restrict social media just as it has other addictive substances like alcohol and tobacco. The design features of social media—aggressive algorithms, "likes," infinite scroll, and constant notifications—make it act like a highly addictive substance for children's developing brains. The de facto age for social media has been low at thirteen years old because of the Children's Online Privacy Protection Act (COPPA). COPPA, however, doesn't restrict minors' access to sites or platforms, it requires parental consent for sites to collect information from children under thirteen. Social media platforms set their age limit to thirteen in order to easily comply with COPPA. But in reality, the platforms don't effectively enforce this age limit, they ignore COPPA, so eight- to twelve-year-olds are on these apps, as recent lawsuits by state attorneys general have publicly exposed.[43]

Congress should ban social media for minors by raising the age at which they can create social media accounts to 16 or 18 years old, in the same way that federal laws have set twenty-one as the minimum age for tobacco or alcohol purchase, and include age-verification requirements so that the age limit is effectively implemented. Restricting social media entirely

42 *TikTok v. Anderson*, United States Court of Appeal for the Third Circuit, No. 22-3061, Judge Paul Matey, Concurring Opinion, August 27, 2024, https://www2.ca3.uscourts.gov/opinarch/223061p.pdf

43 *State of Arizona et al. v. Meta Platforms et al.*, No. 4:23-CV-05448 (N.D. Calif. 2023), oag.ca.gov/system/files/attachments/press-docs/Less-redacted%20complaint%20-%20released.pdf; "Attorney General Bonta: Unredacted Federal Lawsuit Against Meta 'Damning,' " Office of the Attorney General, State of California Department of Justice, November 27, 2023,oag.ca.gov/news/press-releases/attorney-general-bonta-unredacted-federal-lawsuit-against-meta-%E2%80%9Cdamning%E2%80%9D.

for minors under a certain age is a critical collective solution that is needed to help individual parents and families effectively protect their children from the harms of social media.

With a ban, parents wouldn't have to fight the constant battle of saying no to social media for their kids, because it would be a non-option, the same way cigarettes for kids is now a non-option. Parents would no longer have to face societal peer pressure to give their child social media or fear their child's social isolation by not giving, since all kids would simply not be allowed on by law. Bans help everyone keep kids safe.

2. App Store Age Verification and Parental Consent

App stores act as the gatekeepers to the online world and the app ecosystem, they should be responsible for their role in facilitating children's access to harmful digital content, like social media apps and adult apps. Currently, without any accountability, these virtual stores are marketing a myriad of goods that are unsuitable for children, even when parents have enabled app age-rating restrictions on their children's devices. One mom I interviewed for my book shared that even though she has her child's device set up to allow him to have only apps rated nine-plus, whenever she opens the Apple App Store for her ten-year- old, it tells him that his must-have apps are Tinder, TikTok, Hinge, and Bumble. None of these are age-appropriate.

Sadly, the promotions are working. According to one study, one in four nine-to twelve-year-old boys reported they've been on an online dating app.[44]

Congress should pass a law requiring app stores at the device-level to verify the age of the device user when setting up the device/app store ID and then for minor users require a parent account to be linked to the minor's account and require parental consent to access the device app store and parental consent for each instance of an app download or in-app purchase from the app store. Senator Lee and Representative John James introduced such legislation in the 118th Congress, called the App Store Accountability Act, and plan to do so again. I hope others will join them in helping to get this critical legislation passed. The state of Utah recently passed such a law at the state level and many other states have introduced similar bills. Parents must be in the driver's seat over children's app use.

3. Age Verification for Pornography Websites

Congress should pass a federal age-verification law for pornography websites. Nineteen states have now passed age-verification laws for pornography websites. Congress should build on this momentum and provide a federal solution to protect children nationwide, not just state by state, to require platforms that in the regular course of their trade or business, create, host, or make available material that is harmful to minors, to adopt and operate age-verification measures to ensure minors do not access their obscene content or otherwise face legal liability. The status quo of filters has not been enough to advance the government's interest in protecting children from porn. Age-verification laws add an important layer of protection over and beyond what filters can offer. We don't take children to casinos and strip clubs and try to blindfold their eyes or have them wear earplugs. Instead, we simply don't let them go to those places at all. It should be the same for the virtual world. Kids should not be allowed inside of porn websites. Parents need this help.

4. Greater legal liability for online platforms

There are several ways that greater liability could be opened up against social media platforms. First, Section 230 could be reformed by adding a Bad Samaritan carve-out so that if an internet company is

44 "Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking in 2021," Thorn, February 2023, info.thorn.org/hubfs/Research/Thorn_ROT_Monitoring_2021.pdf.

acting like a Bad Samaritan by knowingly promoting criminal content or facilitating criminal behavior, then they don't get to benefit from Section 230 immunity. The bipartisan EARN IT Act that has been introduced in the past would help solve for one area of impunity for the criminal content of child sexual abuse material (CSAM) being distributed on social media by creating a targeted carve-out in Section 230 to remove platforms' immunity from CSAM laws.

Second, Congress could also further empower existing enforcement authorities like the Federal Trade Commission (FTC) and states attorneys general with greater tools to hold tech companies accountable. Changes in federal law could strengthen ongoing lawsuits and encourage more litigation efforts by creating new design requirements for tech companies to keep children safe while using their products. For example, Congress could pass legislation to create new liabilities for tech companies, like product design requirements to mitigate certain objective harms to children. Such legislation could open companies up to litigation for design harms that Section 230 wouldn't be able to get them out of.

Finally, Congress could also empower more FTC enforcement actions against app stores and apps, like social media, by amending the Federal Trade Commission Act's prohibition against "unfair or deceptive acts or practices" to add an explicit prohibition against online platforms, app stores, and apps from abusively marketing their goods to children and from deceptively age rating their apps.

5. Protective Guardrails on AI

The revolution in artificial intelligence has sparked an explosion of "deep fakes," as teens are creating their own obscenity. They no longer need to go looking for porn, they can create their own with AI. Child-safety investigators have also seen an increasing amount of disturbingly lifelike images showing child sexual exploitation, that they fear will undermine efforts to determine real victims and combat real-world abuse. Congress needs to be proactive in putting proper guardrails on AI so that it does not result in technologies that will harm children.

It is critical that Congress helps clarify for Courts that generative AI and the products the AI produces are not to be treated as speech but product design. This is not the speech of the companies, they are not choosing to express themselves or a specific message through what the AI outputs to users, and so should not be protected by the First Amendment for its harms, and neither is it user-generated, third-party speech hosted by the AI, like other online platforms, and so it should also not be protected by Section 230. The outputs may be in the form of human language, but it is not a human's speech, these are computer-generated products from the AI model and the AI itself is not a person with a message to convey. Instead the outputs of AI must be treated as product design. When an AI chatbot tells a 14-year-old "Please come home to me as soon as possible, my love" and leads him to commit suicide by shooting himself in the head, after the bot told him it loved him, engaging in sexual conversation over the course of weeks and months and expressing a desire to be together romantically, the company should be liable for that wrongful death.[45]

One option is for Congress to remove Section 230 liability protection for generative AI. The reasoning is that Section 230 should not apply to generative AI, because the AI is not a platform hosting third-party content, but it is generating and producing its own content drawing from the data set and sources it selects and trains the model on. Clarifying for courts that AI companies should face legal liability for harms to consumers from its product design would help channel the development of AI in productive directions, rather than criminal ones, and help to prevent harms to consumers, especially children, like AI-generated child sexual abuse material.

[45] Angela Yang, "Lawsuit claims Character.AI is responsible for teen's suicide," NBC News, October 23, 2024, https://www.nbcnews.com/tech/characterai-lawsuit-florida-teen-death-rcna176791

Another approach is criminalizing the publication of "deep fake" sexual images, created with AI, on social media, as the bipartisan "Take it Down Act" that has already unanimously passed the Senate, does.[46] The bill makes it unlawful for a person to knowingly publish or threaten to publish non-consensual intimate imagery (NCII), which includes realistic, computer-generated pornographic images and videos that depict identifiable, real people, to social media and other online platforms. It would also require websites to take down such imagery upon notice from the victim within 48 hours.

Congress could also pass a very simple and narrow law that says generative AI may not produce obscenity and child pornography, which are not forms of protected speech, but rather are criminal content. This would help prevent AI from being used by teens to produce their own pornography and prevent pedophiles from using AI to produce child pornography.

I would welcome the opportwunity to work with Congress on any of these proposed solutions. Thank you for your time and I look forward to your questions.

46 https://www.commerce.senate.gov/services/files/A42A827D-03B5-4377-9863-3B1263A7E3B2

Clare Morell is a fellow at the Ethics and Public Policy Center, where she directs EPPC's Technology and Human Flourishing Project. Prior to joining EPPC, Ms. Morell worked in both the White House Counsel's Office and the Department of Justice, as well as in the private and non-profit sectors. She is also the author of the forthcoming book, *The Tech Exit: A Practical Guide to Freeing Kids and Teens from Smartphones*, which will be published by Penguin Random House.