CENTER FOR DEMOCRACY & TECHNOLOGY

Testimony of Kate Ruane
Director of the Free Expression Project, Center for Democracy & Technology

For the U.S. House of Representatives Energy & Commerce Committee
Subcommittee on Commerce, Manufacturing, & Trade
Hearing Entitled "Legislative Solutions to Protect Children and Teens Online"

December 2, 2025

Thank you, Chair Bilirakis, Ranking Member Schakowsky, Chair Guthrie, and Ranking Member Pallone for the opportunity to testify today on the importance of protecting and empowering kids and families online.

I am Kate Ruane, the Director of the Free Expression Project at the Center for Democracy & Technology (CDT), a nonprofit, nonpartisan organization that defends civil rights, civil liberties and democratic values in the digital age.[1] For three decades, CDT has advocated for Congress to adopt strong privacy protections and protect free expression online for everyone, adults and children alike. CDT supported both the American Data Privacy Protection Act (ADPPA) and the American Privacy Rights Act (APRA) as reasonable compromises that would have protected everyone's privacy. These were important pieces of legislation spearheaded by this Committee, which has long demonstrated its commitment to ensuring everyone in the United States can access and use technology they can trust.

Children today will use online services, from web browsers, to social media, to search engines, to chatbots, for their entire lives. The best path forward to protecting children and everyone online and to addressing root causes of many of the concerns related to minors' activities on social media and other online services would be to enact comprehensive consumer data privacy legislation that meaningfully realigns incentives for the business models of covered services. In the absence of comprehensive protections for everyone, all stakeholders, including families, companies, civil society, academics, researchers, technologists, and policy makers, must work together to ensure that young people can grow and learn to use online services in a safe and age-appropriate fashion, regardless of

[1] This testimony is based on the work and insights of numerous experts within CDT, including Samir Jain, Eric Null, Michal Luria, Aliya Bhatia, Nick Doty, Travis Hall, and Kristin Woefel.

their race, gender, socioeconomic status, disability, or familial situation. The subcommittee is right to focus on this critical topic. Our collective future depends on it.

The efficacy of the legislation the Committee today considers further depends on the efficacy of the agency and actors entrusted to enforce the law. All of the bills under consideration task the Federal Trade Commission (FTC) with enforcement or implementation powers. The current Administration is undermining the independence of the FTC, by purporting to "fire" several independent commissioners without cause, contrary to law and the Supreme Court's 1935 decision in *Humphrey's Executor v. United States*.[2] The current chair has even taken to calling his agency the "Trump-Vance FTC," signifying who is really in charge. These actions threaten the FTC's ability to enforce the law fairly, the short and long term implications of which should be of bipartisan concern. Laws without meaningful and fair enforcement mechanisms are at best just words on a page. At worst, they are political weapons that can be wielded by those who hold power against those who do not. As the Committee considers the weighty issues of protecting children online, it must also work to ensure that the agency empowered to execute its policies will do so fairly and in a manner that protects all children and supports the rule of law.

Today I'd like to raise five critical points essential to protecting children online:

1. **Congress should address root causes of online harms including, in particular, privacy.**
2. **Protecting children includes protecting their right to express themselves online.**
3. **Age assurance and verification create significant privacy risks that should be mitigated in legislation if the government requires or incentivizes its use.**
4. **Creating good policy requires taking into account the varied perspectives and experiences of minors and their caregivers.**
5. **Congress must not unduly restrict states' ability to act – and, in particular, must reject any false deal that conditions kids' online safety on preempting states' ability to regulate AI.**

[2] *Humphrey's Executor v. United States*, 295 U.S. 602 (1935).

## I. Congress should address root causes of online harms including, in particular, privacy.

Congress should be mindful not to place legislative bandaids over larger issues. Constitutional concerns discussed below aside, blocking or restricting minors' access to social media or "harmful content" does not address the larger issues underlying the reported increase in youth mental health problems or the surveillance capitalism business model driving many of the content-related concerns expressed by legislators, minors, and their caregivers. To the extent possible, Congress should focus on addressing the root causes of these problems to improve children's lives both online and off. That requires passing privacy legislation.

Currently, many online services' business models are largely based on advertising sales powered by platforms' collection and use of personal information, leading to an overreliance on immediate engagement metrics as a proxy for user-preference and value.[3] This business model is both harmful and deficient. It is harmful because it is privacy invasive and increases the risks of data breaches and inappropriate government access to people's private thoughts.[4] It is deficient because it ignores more durable signals of what is valuable to users about social media and other online services.[5]

Congress could disrupt and realign this business model in a way that would benefit not just children, but everyone who uses internet-enabled services. This Committee has been a leader in demonstrating what meaningful change to consumer data privacy protections could look like. The American Privacy Rights Act (APRA) from last Congress included data minimization provisions that would have required companies to justify their data collection and processing as being "necessary, proportionate, and limited to provide or maintain . . . a specific product or service requested by the

[3] KGI Expert Report, *Better Feeds: Algorithms That Put People First* at iv, Knight Georgetown Inst. (March 2025), https://kgi.georgetown.edu/wp-content/uploads/2025/02/Better-Feeds_-Algorithms-That-Put-People-First.pdf.
[4] FTC Staff Report, *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services*, FTC (Sept. 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf; Justin Sherman, *Data Brokers and Data Breaches*, Duke Sanford Sch. of Pub. Pol'y (Sept. 27, 2022), https://techpolicy.sanford.duke.edu/blogroll/data-brokers-and-data-breaches/.
[5] KGI Expert Report, *supra* note 3.

individual to whom the data pertains" or for a list of other enumerated permissible purposes.[6] These data minimization protections were designed to better match consumer expectations with reality.[7] Specifically, consumers expect companies to collect and use data that is required to provide the service with which they are interacting. APRA would also have provided additional opt-in consent protections for transfers of "sensitive covered data," with additional restrictions on permissible purposes for use, retention, and transfer of specific highly personal types of sensitive data such as biometric and genetic information.[8]

Enacting data minimization would mark a fundamental change to our current data ecosystem, which is currently characterized more by data maximization. Companies have incentives to collect and hoard massive amounts of data to develop detailed individual profiles to target advertising, to train AI systems, and just in case it becomes useful for some other purpose. Those large data stores become targets for hackers and data breaches that result in downstream harms like identity theft, reputational damage, or some other type of injury.[9] State privacy laws have not filled that gap for the most part, as most state laws allow companies to continue setting their own rules with little accountability.[10] Maryland is a notable exception, whose privacy law requiring strict necessity for sensitive data collection just went into effect in October. Privacy legislation, including a strong data minimization provision, would do the most to reduce and realign incentives for data collection and many of the practices that can lead to harms to children (and all users).

While a federal law providing comprehensive privacy protections to everyone is the preferable path, enhancing children's privacy protections is also a laudable goal. For more than twenty-five years, the Children's Online Privacy Protection Act (COPPA) has been the primary vehicle for protecting

---

[6] American Privacy Rights Act, H.R. 8818 (118th Cong., 2d session), https://www.congress.gov/bill/118th-congress/house-bill/8818/text.

[7] *See generally* Colleen McClain, Michelle Faverio, Monica Anderson, & Eugenie Park, *How Americans View Data Privacy*, Pew Rsch. Ctr. (Oct. 2023), https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-privacy-laws/.

[8] CDT supported APRA only prior to the removal of its civil rights and algorithmic transparency provisions.

[9] Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 Boston U. L. Rev. 793 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222.

[10] Eric Null, *States Are Letting Us Down on Privacy*, Ctr. for Democracy & Tech. (Jan 28, 2024), https://cdt.org/insights/states-are-letting-us-down-on-privacy.

children's privacy online.[11] We were pleased to see H.R. 6291, the Children and Teens' Online Privacy Protection Act, a long-planned update to COPPA known as "COPPA 2.0," on the agenda for consideration today. CDT has been involved in numerous discussions to refine this legislation to improve privacy protections for kids and teens online and to ensure it does not infringe on the First Amendment.

However, this version of COPPA 2.0 raises new concerns around weakening existing privacy protections for minors, similar to the concerns raised by the new version of KOSA discussed below and in Section V of this testimony. The bill would preempt "any law, rule, regulation, requirement, standard, or other provision having the force and effect of law that relates to the provisions of this Act."[12] This preemption standard will very likely lead to unintended and harmful outcomes by preventing the enforcement of state privacy laws that provide protections beyond those that COPPA would offer. In particular, this standard would weaken existing state privacy laws that protect children's data as "sensitive data," which is often subject to enhanced protections under these laws. Rather than adopting broad "related to" preemption, the House should change the preemption language in COPPA 2.0 to preempt only "conflicting" state law, to avoid extensive litigation around what state protections might "relate to" the new COPPA and to ensure COPPA maximizes protections available to children at the state and federal level.[13] We hope to work with Representatives Walberg and Lee as well as Senators Markey and Cassidy, COPPA 2.0's main Senate sponsors, to ensure COPPA 2.0 improves and adds to the kids' privacy landscape and avoids unintended consequences.

CDT also appreciates H.R. 6292, the "Don't Sell Kids' Data" Act. This bill would generally prohibit data brokers from collecting, selling, or transferring the personal data of someone they know is a child or teen and would empower families with a private right of action to enforce the prohibition and

[11] 15 U.S.C. §§ 6501-6506.
[12] Children and Teens' Online Privacy Protection Act, H.R. 6291 (119th Cong. 1st. Sess.), https://docs.house.gov/meetings/IF/IF17/20251202/118714/BILLS-119HR6291ih.pdf.
[13] *See* Children and Teens' Online Privacy Protection Act, S. 836 (119th Cong.) ("The provisions of this title shall preempt any State law, rule, or regulation only to the extent that such State law, rule, or regulation conflicts with a provision of this title. Nothing in this title shall be construed to prohibit any State from enacting a law, rule, or regulation that provides greater protection to children or teens than the provisions of this title."), https://www.congress.gov/bill/119th-congress/senate-bill/836.

ensure it is meaningful. Data brokers are uniquely harmful actors in the online monetization ecosystem. Mitigating the harm they cause to children and the risks of the exposure of children's data to bad actors is a worthy goal, which CDT supports.

## II. Protecting children includes protecting their right to express themselves online.

Protecting children online is not just about protecting them from harm. It is also about protecting their ability to use technology to express themselves, gather information, and communicate with their peers, parents, families, and friends. An estimated 5.66 billion people use social media as of October 2025.[14] Many of the experiences that people, including minors, have on social media are positive. Minors use social media to access news,[15] organize and engage in protests,[16] discuss politics, learn about art, history and other topics,[17] and to create art themselves. One study reported that "[i]n any given day, about one in 10 tweens and teens will use their digital devices to create some type of art or music."[18] Many minors also report that social media and online spaces can be important places for them to find community, form their identities, and receive support that may not be available to them offline.[19] Preserving youth's access to these spaces and their ability to exercise their free expression

[14] *See* Christy Tila, *Number of Internet and Social Media Users Worldwide as of October 2025*, Statista (Nov. 19, 2025), https://www.statista.com/statistics/617136/digital-population-worldwide/?srsltid=AfmBOorRBPr9l2O3OK2HAUpbP1Lsi4WBrnc83N16ip_gB1X9Fl2sYHqZ.
[15] Christopher St. Aubin & Jacob Liedke, *Social Media and News Fact Sheet*, Pew Rsch. Ctr., (Sept. 25, 2025), https://www.pewresearch.org/journalism/fact-sheet/social-media-and-news-fact-sheet/; Michelle Faverio & Olivia Sidoti, *Teens, Social Media and Technology 2024*, Pew Rsch. Ctr. (Dec. 12, 2024), https://www.pewresearch.org/internet/2024/12/12/teens-social-media-and-technology-2024/; Kerry Flynn, *How Gen Z Gets its News*, Axios (Feb. 16, 2024), https://www.axios.com/2024/02/16/tiktok-news-gen-z-social-media.
[16] Megan Carnegie, *Gen Z: How Young People Are Changing Activism*, BBC News (Aug. 8, 2022), https://www.bbc.com/worklife/article/20220803-gen-z-how-young-people-are-changing-activism.
[17] Jason Kelley, *Thousands of Young People Told Us Why the Kids Online Safety Act Will Be Harmful to Minors*, EFF (Mar. 15, 2024), https://www.eff.org/deeplinks/2024/03/thousands-young-people-told-us-why-kids-online-safety-act-will-be-harmful-minor.
[18] Victoria Rideout, *et al.*, *The Common Sense Census: Media Use by Tweens and Teens 2021* at 41, Common Sense Media (2021), https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf.
[19] Kaitlin Tiches, *The Online Experiences of LGBTQ+ Youth*, Boston Children's Digit. Wellness Lab (Jan. 2025), https://digitalwellnesslab.org/research-briefs/the-online-experiences-of-lgbtq-youth/; Claire Cain Miller, *For One Group of Teenagers, Social Media Seems a Clear Net Benefit*, N.Y. Times (May 24, 2023), https://www.nytimes.com/2023/05/24/upshot/social-media-lgbtq-benefits.html; Asaka Park, *I'm a Disabled Teenager, and*

rights online, even as the Committee works to improve safeguards against harm, is part and parcel of protecting kids online.

Minors' ability to engage and speak online is not only a normative value that supports their rights and development. It is also a constitutional mandate. A long line of precedent establishes that children have First Amendment rights and "only in relatively narrow and well-defined circumstances may government bar public dissemination of protected materials to them."[20] For example, in *Brown v. Entertainment Merchants Association*, the Supreme Court struck down a California statute restricting the sale of violent video games to minors. In that decision, the Court noted, "No doubt a State possesses legitimate power to protect children from harm, [...], but that does not include a free-floating power to restrict the ideas to which children may be exposed."[21] The Seventh Circuit, reviewing a similar ban on minors' access to violent video games, explained, "[minors] must be allowed the freedom to form their political views on the basis of uncensored speech before they turn eighteen, so that their minds are not a blank when they first exercise the franchise."[22] The court reasoned that "[t]o shield children right up to the age of 18 from exposure to [disfavored or harmful ideas] would not only be quixotic, but deforming; it would leave them unequipped to cope with the world as we know it."[23]

It is our task to assist minors in the process of becoming adults who are capable of navigating online services and digital tools, to ensure they are not "a blank" when they first encounter these services, shocked and confused by the content that they encounter. To do so, we must work to protect them from harm in a manner that respects constitutional limitations, and we must also protect their rights. The government and social media platforms should not be — indeed, with respect to the government, *cannot be* — the sole arbiters of the content children can see and services that they can access online. Substituting the judgment of the government or of social media corporations for the

---

*Social Media Is My Lifeline*, N.Y. Times (Jun. 5, 2019), https://www.nytimes.com/2019/06/05/learning/im-a-disabled-teenager-and-social-media-is-my-lifeline.html.

[20] *Brown v. Ent. Merchs. Ass'n,* 564 U.S. 786, 794 (2011) (quoting *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 212-13 (1975)).

[21] *Id*. at 794.

[22] *Am. Amusement Mach. Ass'n v. Kendrick*, 244 F.3d 572, 577 (7th Cir. 2001).

[23] *Id*.

judgment of minors and their caregivers about what content is appropriate for them to view or engage with will lead to censorship, especially of controversial or poorly understood topics, including speech related to LGBTQ issues, firearms, and issues that might increase anxiety like news coverage of armed conflict or climate change.[24] Bills like the current Senate version of the Kids Online Safety Act (KOSA) and the Kids Off Social Media Act (KOSMA),[25] which has become the Reducing Exploitative Social Media Exposure for Teens (RESET) Act[26] in the House, commit precisely this error.

The Senate version of KOSA would require covered online services to exercise reasonable care in the creation and implementation of any design feature to prevent and mitigate enumerated harms such as "depressive disorders and anxiety disorders," yet the factors that drive these disorders are varied, complex, and extend well beyond kids' online environments.[27] Senate KOSA would require platforms to make speculative judgments about how certain constitutionally-protected content and design features may contribute to these outcomes and how best to prevent them — and put the government in charge of adjudicating whether platforms guessed right. But parents and their children — not platforms or governments — are best positioned to make these important choices and, indeed, have a constitutionally-protected right to do so.[28]

This Committee through Chair Bilirakis's leadership has rightly recognized that this approach, while well-intentioned, gives too much power to the government to decide what ideas children should

---

[24] *See, e.g.*, Brooke Tanner & Nicol Turner Lee, *Children's Online Safety Laws Are Failing LGBTQ+ Youth*, Brookings Inst. (Jul. 9, 2025), https://www.brookings.edu/articles/childrens-online-safety-laws-are-failing-lgbtq-youth/; Taylor Lorenz, *Instagram Blocked Teens from Searching LGBTQ-Related Content for Months*, User Mag (Jan. 6, 2025), https://www.usermag.co/p/instagram-blocked-teens-from-searching; Daysia Tolentino, *YouTube Is Implementing Stricter Rules Around Gun Videos,* NBC News (Jun. 6, 2024), https://www.nbcnews.com/tech/tech-news/youtube-implementing-stricter-rules-gun-videos-rcna155896.; Daysia Tolentino, *YouTube Is Implementing Stricter Rules Around Gun Videos,* NBC News (Jun. 6, 2024), https://www.nbcnews.com/tech/tech-news/youtube-implementing-stricter-rules-gun-videos-rcna155896.

[25] Kids Off Social Media Act, S. 278 (119th Cong. 1st. Sess.), https://www.congress.gov/bill/119th-congress/senate-bill/278.

[26] Reducing Exploitative Social Media Exposure for Teens Act, H.R. ___ (119th Cong. 1st. Sess.), https://docs.house.gov/meetings/IF/IF17/20251202/118714/BILLS-119pih-HR___RESETAct.pdf.

[27] Kids Online Safety Act, S. 1748 (119th Cong. 1st Sess.), https://www.congress.gov/bill/119th-congress/senate-bill/1748. *See* danah boyd, *KOSA Isn't Designed to Help Kids*, Substack (Jan. 31, 2024), https://zephoria.substack.com/p/kosa-isnt-designed-to-help-kids.

[28] *See Brown*, 564 U.S. at 794; *NetChoice v. Bonta I*, 113 F.4th 1101,1121 (9th Cir. 2024) (upholding a preliminary injunction against the enforcement of a requirement for covered services to assess what content might harm children and take action to address that content because it regulated constitutionally protected speech and did not survive strict scrutiny).

be able to access online and, for that reason, would likely be held unconstitutional, as other similar laws enacted at the state level have been.[29] Legislation more narrowly tailored to address harms that the constitution permits Congress to regulate is more likely to protect children for the simple reason that it will not be overturned. The House version of KOSA has improved on the Senate version by narrowing the duty of care to require covered services to establish, implement, maintain, and enforce reasonable policies to address threats of violence, sexual exploitation and abuse, distribution, sale, or use of narcotic drugs, and financial harm caused by deceptive practices.[30] These categories of content target speech that is more likely to fall outside constitutional protection.[31]

While the new version has moved in the right direction toward protections and safeguards for children online that focus on illegal content,[32] we are concerned that the preemption provision currently included in the bill would sweep more broadly than intended or advisable. For example, it

---

[29] *See NetChoice LLC v. Carr*, 789 F.Supp. 3d 1200 (N.D. Ga. 2025); *NetChoice, LLC v. Yost*, 778 F. Supp. 3d 923 (S.D. Ohio 2025), *appeal docketed*, No. 25-3371 (6th Cir. May 13, 2025); *NetChoice, LLC v. Griffin*, No. 23-5105,2025 U.S. Dist. LEXIS 61278 (W.D. Ark. Mar. 31, 2025), *appeal docketed*, No. 25-1889 (8th Cir. May 2, 2025); *NetChoice, LLC v. Bonta*, 770 F. Supp. 3d 1164 (N.D. Cal. 2025), *appeal docketed*, No. 25-2366 (9th Cir. Apr. 11, 2025); *NetChoice, LLC v. Reyes*, 748 F. Supp. 3d 1105 (D. Utah 2024), *appeal docketed sub nom*., *NetChoice, LLC v. Brown*, No. 24-4100 (10th Cir. Oct. 11, 2024).

[30] Kids Online Safety Act, H.R.___, (119th Cong. 1st Sess.), https://docs.house.gov/meetings/IF/IF17/20251202/118714/BILLS-119pih-HR____KidsOnlineSafetyAct.pdf.

[31] True threats and incitements to violence, child sexual abuse, advertisements for illegal drugs, speech integral to criminal conduct, and deceptive commercial speech are not protected by the First Amendment. *See Counterman v. Colorado*, 600 U.S. 66, 74 (2023) (true threats); *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969) (per curiam) (incitement to violence); *New York v. Ferber*, 458 U.S. 747, 765 (1982) (child sexual abuse material); *Central Hudson Gas & Electric Corp. v. PSC*, 447 U.S. 557, 563 (1980) (advertisements for illegal activity and advertisements that are misleading are not protected speech), *Giboney v. Empire Storage & Ice Co.*, 336 U.S. 490 (1949) (speech integral to criminal conduct).

[32] There also may be lingering constitutional concerns with some of the restrictions included in the pared down version of KOSA. Determining whether particular speech falls outside the ambit of the constitution's protections is a fact-specific endeavor. *See Counterman*, 600 U.S. at 73 (recounting tests for unprotected speech); *Central Hudson*, 447 U.S. at 563 (describing false commercial speech as unprotected). When applying restrictions on the distribution of content, even illegal content, courts have been wary of the chilling effects the application of liability to distributors of speech might have. *See Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 71 (1963). KOSA's duty of care, even the pared down version currently before the House, requires covered services to make judgments about what content should be covered by its policies often based upon imperfect information and potentially no information regarding the original speaker's intent. Mike Masnick, *Masnick's Impossibility Theorem: Content Moderation at Scale Is Impossible To Do Well*, TechDirt (Nov. 20, 2019) ("[T}o to make good decisions you often need a tremendous amount of context, and there's simply no way to adequately provide that at scale in a manner that actually works.") https://www.techdirt.com/2019/11/20/masnicks-impossibility-theorem-content-moderation-scale-is-impossible-to-do-well. In addition, covered services will likely use filtering technologies that are necessarily imperfect to comply with the statute. *See* Natasha Duarte, *et al*., *Mixed Messages? The Limits of Automated Social Media Content Analysis*, Ctr. for Democracy & Tech. 6 (Nov. 2017), https://cdt.org/wp-content/uploads/2017/11/Mixed-Messages-Paper.pdf. This leaves questions about whether the duty of care will work as a prior restraint on protected speech, raising constitutional concerns.

could preempt protections enacted at the state level for children interacting with chatbots, even though KOSA would not apply to minors' use of chatbots. We hope to work with the Committee to resolve these concerns.

The RESET Act, H.R. ___, is more concerning than both the House and Senate versions of KOSA from a constitutional perspective. The RESET Act would ban all users under 16 from creating an account on social media services, including ones with appropriate safeguards. As noted above, eliminating minors' access to social media accounts would cut them off from online expression, political engagement, and essential educational resources on services like YouTube, Pinterest, and Reddit. At a time when books are being banned in schools and curricula are being restricted,[33] ensuring young people can access a broad range of perspectives online — and a broad community — is more critical than ever. The RESET Act, however, would shut kids under 16 off from this world, in violation of the First Amendment and contrary to the interests of this Committee in protecting minors. Courts have already enjoined numerous state laws that attempted to enact similar restrictions for likely violating the First Amendment.[34]

## III. Age assurance and verification create significant privacy risks that should be mitigated in legislation if the government requires or incentivizes its use.

KOSA and the RESET Act, as well as many of the other bills under consideration today, either require or incentivize covered services to verify the ages of their users in order to identify which users are minors and therefore be able to comply with the law. There are at least two broad concerns with government requirements — whether explicit or implicit — to conduct age assurance.[35] The first is

[33] Sabrina Baêta, *et al*., *The Normalization of Book Banning*, PEN America (Oct. 1, 2025), https://pen.org/report/the-normalization-of-book-banning/.

[34] *See NetChoice LLC v. Carr*, 789 F.Supp. 3d 1200 (N.D. Ga. 2025); *NetChoice, LLC v. Yost*, 778 F. Supp. 3d 923 (S.D. Ohio 2025), *appeal docketed*, No. 25-3371 (6th Cir. May 13, 2025); *NetChoice, LLC v. Griffin*, No. 23-5105, 2025 U.S. Dist. LEXIS 61278 (W.D. Ark. Mar. 31, 2025), *appeal docketed*, No. 25-1889 (8th Cir. May 2, 2025); *NetChoice, LLC v. Bonta*, 770 F. Supp. 3d 1164 (N.D. Cal. 2025), *appeal docketed*, No. 25-2366 (9th Cir. Apr. 11, 2025); *NetChoice, LLC v. Reyes*, 748 F. Supp. 3d 1105 (D. Utah 2024), *appeal docketed sub nom*., *NetChoice, LLC v. Brown*, No. 24-4100 (10th Cir. Oct. 11, 2024).

[35] This testimony will use age assurance as an umbrella term to refer to all techniques to determine the age of users of online services. It will use age verification to refer to techniques that assess age based upon government issued identifiers. It will use age estimation to refer to techniques that assess age on the basis of biometric scans, company-held data, or other methods that do not require the provision of a government ID.

legal. Age assurance requirements often place burdens on access to speech for adults and children alike, and, as the Supreme Court recently reiterated, that means the First Amendment applies.[36] The second is practical. Currently available age assurance methods may have improved upon past iterations of the technology, but they have not eliminated the privacy and efficacy concerns raised by their use, as forthcoming research from experts at Georgia Institute of Technology will demonstrate, and can likely never do so because conducting age assurance will almost invariably require more data collection and processing than would otherwise be necessary.[37] If the government is going to mandate the use of such tools to access online services, at a minimum, certain safeguards must be included in those mandates to mitigate privacy risks and chilling effects on access to constitutionally protected speech.[38]

### A. Legal Concerns with age assurance requirements

Recently, the Supreme Court, in *Free Speech Coalition v. Paxton*, upheld an age verification requirement against constitutional challenge.[39] Under that case, states and the federal government are allowed to require age verification for the purposes of accessing content that is obscene for minors online. In its opinion, the Court reasoned that minors do not have the constitutional right to access such content and therefore everyone, both adults and minors, can logically be required to submit to age verification in order to effectuate a ban on minors' access. While the First Amendment did apply to the imposition of age assurance in this context, the Court held that it was an incidental restriction on speech and therefore permissible.

However, the decision should be construed to sweep no more broadly than that. It included important limiting language regarding the scope of what can be considered "obscene" for minors and therefore subject to age gating. The *FSC* Court reiterated that content that is obscene as to minors

---

[36] *Free Speech Coalition v. Paxton*, 606 U.S. 461, 478 (2025) (hereinafter "*FSC*") (holding that age verification requirements burden adults' access to content they have a constitutional right to view and must withstand First Amendment review).
[37] *See* Shreyas Minocha, Isaac Sheridan, Harry Oppenheimer, Paul Pearce, & Michael Specter, *Papers, Please: A First Look at Age Verification on the Web.* Georgia Inst. of Tech. (forthcoming).
[38] Aliya Bhatia & Nick Doty, *Mitigating Risk to Rights with Age Verification: Privacy-Preserving Guardrails that Should Accompany Deployments of Age Verification Approaches*, Ctr. for Democracy & Tech. (Oct. 10, 2025), https://cdt.org/insights/mitigating-risk-to-rights-with-age-verification-privacy-preserving-guardrails-that-should-accompany-deployments-of-age-verification-approaches/.
[39] *FSC,* 606 U.S. at 465.

includes only "works that (a) taken as a whole, and under contemporary community standards, appeal to the prurient interest of minors; (b) depict or describe specifically defined sexual conduct in a way that is patently offensive for minors, and (c) taken as a whole, lack serious literary, artistic, political, or scientific value for minors."[40] As to what kind of content that might entail, a previous Supreme Court case, *Ginsberg v. New York*, had found that "girlie magazines," like Playboy, could be considered to fall in this category.[41] The *FSC* Court in a footnote gave additional guidance illustrating how limited this category of speech is, explaining that it "cannot conceivably be read to cover, say, a PG-13 or R Rated movie."[42] The Court was very clear in its reasoning that it was upholding the state statute at issue because it barred minors' access to content they do not have the constitutional right to view, and the burden it placed on the speech of adults was tailored to service the goal of restricting access to that narrow category of content by minors.

Laws creating age assurance burdens for adults and children to access content that is not obscene for minors were not addressed in *FSC v. Paxton*, and earlier precedent holds that these types of laws should receive the highest degree of scrutiny a court can apply—in part because they would significantly burden adults' constitutional rights, in addition to unconstitutionally infringing on children's speech rights.[43] Where age assurance requires the provision of government identification, the requirement "serve[s] as a complete block to adults who wish to access [gated] material [online] but do not" have or wish to provide government identification to do so.[44] The number of people lacking identification is significant: according to the Center for Democracy and Civic Engagement, 21 million people do not have a current (non-expired) drivers' license.[45] Non-identification-based methods also create barriers to access for adults. For example, methods relying on mortgage data exclude adults that

[40] *Id*. at 472.
[41] *Ginsberg v. New York*, 390 U.S. 629, 634 (1968).
[42] *FSC,* 606 U.S. at 481 n.7.
[43] *Ashcroft v. ACLU*, 542 U.S. 656 (2004); *Reno v. ACLU*, 521 U.S. 844 (1997).
[44] *PSINet, Inc. v. Chapman*, 362 F.3d 227, 237 (4th Cir. 2004). *See also Reno*, 521 U.S at 856 (1997) (noting that requiring credit card information to verify age would serve as a complete bar to users who lacked a credit card).
[45] Jillian Andres Rothschild, *et al*., *Who Lacks ID in America Today? An Exploration of Voter ID Access, Barriers, and Knowledge* at 2, Univ. Md. Ctr. for Democracy & Civic Engagement (Jan. 2024), https://cdce.umd.edu/sites/cdce.umd.edu/files/pubs/Voter%20ID%202023%20survey%20Key%20Results%20Jan%202024%20%281%29.pdf.

do not own a home.[46] Methods relying on credit card data also exclude Americans who do not have a credit card, particularly young adults who are often "credit invisible."[47] Each of these methods also significantly compromises the privacy with which adults can access information online.

Thus, while the Supreme Court has ruled that Congress may now require age assurance to access material that is obscene as to minors, age assurance requirements that sweep more broadly than that to erect barriers to access social media services or reduce access to certain content or features that are constitutionally protected for everyone remain constitutionally suspect.[48] A number of courts have enjoined state social media bans and age appropriate design codes resembling Senate KOSA.[49] While some appeals courts have stayed or vacated preliminary injunctions against some state social media bans,[50] Justice Kavanaugh's concurrence in *NetChoice v. Fitch* expressing doubts about the constitutionality of social media bans indicates that the Supreme Court might not uphold their reasoning.[51] Accordingly, as this Committee has paid close attention to KOSA to shore up its constitutionality, it should do the same for other bills which would erect age assurance barriers to access constitutionally protected speech online.

### B. Practical Considerations for age assurance implementation

To the extent that the government is now permitted to impose age assurance requirements for accessing certain content, setting aside potential constitutional issues, age assurance techniques

---

[46] *See Reno*, 521 U.S at 856.
[47] *Id*. *See also* Kenneth P. Brevoort, *et al.*, *Data Point: Credit Invisibles* at 12, Consumer Fin. Prot. Bureau (May 2015), https://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf.
[48] Kate Ruane & Aliya Bhatia, FSC v Paxton *Made Bad Law, But It's Not Carte Blanche for Age Verification*, Cntr. for Democracy & Tech (Aug. 22, 2025), https://cdt.org/insights/fsc-v-paxton-made-bad-law-but-its-not-carte-blanche-for-age-verification/.
[49] *See NetChoice LLC v. Carr*, 789 F.Supp. 3d 1200 (N.D. Ga. 2025); *NetChoice, LLC v. Yost*, 778 F. Supp. 3d 923 (S.D. Ohio 2025), *appeal docketed*, No. 25-3371 (6th Cir. May 13, 2025); *NetChoice, LLC v. Griffin*, No. 23-5105, 2025 U.S. Dist. LEXIS 61278 (W.D. Ark. Mar. 31, 2025), *appeal docketed*, No. 25-1889 (8th Cir. May 2, 2025); *NetChoice, LLC v. Bonta*, 770 F. Supp. 3d 1164 (N.D. Cal. 2025), *appeal docketed*, No. 25-2366 (9th Cir. Apr. 11, 2025); *NetChoice, LLC v. Reyes*, 748 F. Supp. 3d 1105 (D. Utah 2024), *appeal docketed sub nom*., *NetChoice, LLC v. Brown*, No. 24-4100 (10th Cir. Oct. 11, 2024).
[50] *See Comput. & Commc'ns Indus. Ass'n v. Uthmeier*, No 25-11881 (11th Cir. 2025), https://netchoice.org/wp-content/uploads/2025/11/11th-Circuit_CCIA-NetChoice-v.-Uthmeier_HB-3_Ruling_Nov-25-2025.pdf; *NetChoice, L.L.C. v. Fitch*, 134 F.4th 799 (5th Cir. 2025).
[51] *NetChoice v. Fitch*, 606 U. S. ____ (2025) (Kavanaugh, J., concurring in the denial of an application to vacate stay), https://www.supremecourt.gov/opinions/24pdf/25a97_5h25.pdf.

continue to raise significant concerns for *all* users' privacy and free expression rights.[52] Requiring users to prove their age to access content or services leads to more data collection, processing, and retention by already data-rich services. Just as importantly, users of all ages lose the ability to access the web anonymously when they have to provide proof of age documents or other identity-revealing information beforehand. People go online to access — and speak about— all sorts of sensitive topics such as their health status, religious or political views, whistleblowing, sexuality, and experiences with domestic violence. Users often want to access and share this information privately. Because removing minors' ability to communicate or access content that may be deemed age-inappropriate requires sorting minors from adults, all users' ability to surf the web privately and speak freely is compromised. This is likely to create chilling effects for many users who are reluctant to seek out sensitive and important information to which they don't want to be publicly linked.[53]

Given these and other foreseeable harmful consequences, some services may decide to avoid providing service in jurisdictions with particularly invasive age assurance mandates, obviously negatively impacting the adults in those jurisdictions who would otherwise want to avail themselves of those services. Indeed, Bluesky[54] no longer offers service in Mississippi for this reason — a "significant blow"[55] for Mississippians. Other services, too, have stopped offering service to Mississippi residents, ranging from PornHub,[56] an adult-content website, to Dreamwidth,[57] an open source online journal and blogging community. These jurisdiction-by-jurisdiction decisions lead to increased fragmentation of the

[52] Bhatia & Doty, *supra* note 38.
[53] Aliya Bhatia, *Age Estimation Requires Verification for Many Users*, Ctr. for Democracy & Tech. (Mar. 24, 2025), https://cdt.org/insights/age-estimation-requires-verification-for-many-users/. *See also* Kim Zetter, *Hackers Finally Post Stolen Ashley Madison Data*, Wired (Aug. 18, 2015), https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/.
[54] Megan Farokhmanesh, *Bluesky Goes Dark in Mississippi Over Age Verification Law,* Wired (Aug. 22, 2025), https://www.wired.com/story/bluesky-goes-dark-in-mississippi-age-verification/,
[55] Ashton Pittman, *Bluesky Blocks Mississippi IPs, Citing State's Age Verification Law, Free Speech and Privacy Concerns*, Miss. Free Press (Aug. 22, 2025), https://www.mississippifreepress.org/editors-note-bluesky-blocks-mississippi-ips-citing-states-age-verification-law-free-speech-and-privacy-concerns/.
[56] Jacob Kastrenakes, *Pornhub Blocks Access in Mississippi and Virginia Over Age Verification Laws*, Verge (Jul. 3, 2023), https://www.theverge.com/2023/7/3/23782776/pornhub-blocks-mississippi-virginia-age-verification-laws.
[57] *Mississippi Legal Challenge: Beginning 1 September, We Will Need to Geoblock Mississippi IPs*, Dreamwidth Studios (Aug. 26, 2025), https://dw-news.dreamwidth.org/44429.html.

web, with peoples' experience of the internet differing from state to state, harming users who can no longer access the information, communities, networks, or other capabilities the service offers.

Online safety proposals, including a number of the bills at issue today, often require or incentivize the use of invasive age assurance mechanisms without sufficient safeguards to govern the secondary use, retention, and third-party sharing of this data.[58] Age assurance approaches often require platforms to collect hard identifiers of age (such as government ID) or biometric data from all users as a prerequisite to access the service. This opens the door for vast data collection and retention from users, and risks linking users' identity to their online activity, which itself can be incredibly sensitive. Specifically, biometric data should be treated especially carefully, as it is immutable and easily abused.

Researchers at the Georgia Institute of Technology are about to publish a study providing empirical evidence that the privacy and security concerns related to the use of age verification and assurance techniques are significant and are, indeed, playing out in real time as age assurance requirements take effect.[59] In particular, the study finds that the widespread implementation of age assurance, particularly in states that have implemented age assurance requirements, increases privacy and security risks for end users, can be ineffective, and has increased the balkanization of the internet in the United States for the first time. The researchers further examined one of the dominant third-party age assurance vendors and found that the service can require users to share large amounts of personally identifiable information (e.g., photos of their face, government IDs, credit card information, browser fingerprinting data and more). Moreover, the information is not only shared with the contracted service provider. It is also shared with several "fourth parties" that are not as visible to users. For most age checks, the provider claims data is deleted when the age-check is complete, but, according to the researchers, that is not always the case. For some ID-based checks, for example, the provider may hold data for up to 28-days, including a potential data transfer to India. In short, in popular "commercially reasonable" third-party age assurance provider services, there is almost certainly more data collection, more sharing of that data with additional parties, more cross-border

[58] *See* Bhatia & Doty, *supra* note 38.
[59] Shreyas Minocha, *et al*., *supra* note 37.

data transfers, and longer data retention than many users or the legislators mandating their use would expect or support. The findings of this paper demonstrate that age verification vendors present significant privacy concerns and may not be sufficiently incentivized to maximize user privacy.

These concerns are far from hypothetical. Just this summer, a popular dating safety app was hacked, revealing the personal images and comments of thousands of women. The leak included images of women holding their photo ids for verification purposes, despite the app's claims that such photos were deleted immediately after authentication.[60] Very recently, Discord disclosed that it was subject to a data breach, in which part of the data that was inappropriately accessed by an unauthorized third party was users' IDs provided to Discord as part of the company's process to appeal incorrect age estimations made by the platform's age assurance process.[61] And last year, a leading age verification provider was hacked, allowing users' names, drivers' licenses and nationality to be made available to others on the internet.[62] Without robust privacy controls baked in, age verification mandates significantly increase the risk of such events.

If Congress nevertheless feels obligated to require or incentivize age assurance, it should also require guardrails to mitigate the risks to users' privacy and safety. In particular, Congress should mandate mechanisms for age assurance are:

- proportional and narrowly tailored;
- reliant on high quality sources of data to ensure context-dependent accurate verification;
- nondiscriminatory and uniformly accessible to all;

---

[60] Alana Wise, *Tea Encouraged Its Users to Spill. Then the App's Data Got Leaked*, NPR (Aug. 2, 2025), https://www.npr.org/2025/08/02/nx-s1-5483886/tea-app-breach-hacked-whisper-networks; Emanuel Maiberg & Joseph Cox, *A Second Tea Breach Reveals Users' DMs About Abortions and Cheating*, 404 Media (Jul. 28, 2025), https://www.404media.co/a-second-tea-breach-reveals-users-dms-about-abortions-and-cheating/; Isabella Kwai, *What to Know About the Hack at Tea, an App Where Women Share Red Flags About Men*, N.Y. Times (Jul. 26, 2025), https://www.nytimes.com/2025/07/26/us/tea-safety-dating-app-hack.html.

[61] Discord, *Update on a Security Incident Involving Third-Party Customer Service* (Oct. 3, 2025), https://discord.com/press-releases/update-on-security-incident-involving-third-party-customer-service.

[62] Joseph Cox, *ID Verification Service for TikTok, Uber, X Exposed Driver Licenses,* 404 Media (Jun. 26, 2024), https://www.404media.co/id-verification-service-for-tiktok-uber-x-exposed-driver-licenses-au10tix/.

- private and secure, meaning unlinkable, data-minimized, retention-limited, purpose-restricted, securely-implemented, and not shared or distributed;
- transparent; and
- accountable and remediable.

Age assurance approaches should be proportional and narrowly tailored to the harm they seek to minimize. This means age assurance measures should be required to be implemented as narrowly as possible, particularly on mixed-audience services. For example, if an age assurance mandate applies to adult content and only some content on a site falls in that category, the site should be required to apply age gates to access only the adult content, rather than the entire site.

Age assurance requirements should mandate reliance on high quality sources of data to verify age and ensure accurate verification. The data collected by age assurance providers should vary by context. For example, some providers may already have relevant data about users and need to collect little additional information to verify age; others will have no information. The appropriate degree of accuracy may also vary by the particular risks that verification is intended to protect against.

Additionally, these approaches should be nondiscriminatory and accessible to all users, as demonstrated by periodic audits and pre- and post-deployment testing. User control tools and age verification approaches should be uniformly and consistently available and compatible with different devices and operating systems. This includes ensuring that mechanisms work with parity for all users regardless of their language, age, race, gender, or nationality. Furthermore, it is particularly important that age assurance mechanisms are accessible to people with disabilities, including people who are blind or low-vision, and comply with accessibility standards enshrined within relevant disability rights statutes, including the Americans with Disabilities Act.

Companies, including age assurance vendors, should be required to adhere to clear privacy and security limits to restrict the collection, use, sharing, and retention of the data collected. Age-related data is not only sensitive but also lucrative, making services that collect and store it attractive to data brokers or malicious hackers. Information pertaining to a person's age, date of birth, home address and birthplace, as well as biometric data, is either immutable or difficult to change and therefore

particularly sensitive. In the event of identity theft or improper access, the consequences can be devastating and difficult to address.

Specific data protections should include:

- limiting the collection, sharing, and retention of age-related data for anything other than verifying age;
- preventing any secondary use of data collected for mandatory age verification;
- minimizing or entirely preventing linkability between where users provided age-related data and the issuer of that data — e.g., ensuring that the the entity verifying age does not disclose to the issuer of the ID (for example: a state DMV) which sites the user is accessing;
- declining to collect or store any information not needed to determine the user's age or age range (e.g., if a user provides an ID, the verifier should not collect information such as a social security number or driver's license number as well);
- limiting data retention and deleting data promptly once age or age range has been determined, as the raw data is no longer needed; and
- implementing cybersecurity measures (e.g., encrypting data in transit and storage) to prevent malicious access to or uses of age-related data.

Linking IDs (and all of the information on them) to users' online behavior creates a massive cyber-security and privacy risk.[63] Moreover, the mere spectre of linkability and greater data collection will chill users' inclination to access constitutionally-protected speech, a phenomenon demonstrated in the states and other jurisdictions where age verification laws are already in place and VPN usage has skyrocketed.[64]

---

[63] *See* Jacqui Wakefield, *My Ex Stalked Me, So I Joined a 'Dating Safety' App. Then My Address Was Leaked*, BBC News (Aug. 22, 2025), https://www.bbc.com/news/articles/ce87rer52k3o. *See also* Alana Wise, *Tea Encouraged Its Users to Spill. Then the App's Data Got Leaked*, NPR (Aug. 2, 2025), https://www.npr.org/2025/08/02/nx-s1-5483886/tea-app-breach-hacked-whisper-networks; Emanuel Maiberg & Joseph Cox, *A Second Tea Breach Reveals Users' DMs About Abortions and Cheating*, 404 Media (Jul. 28, 2025), https://www.404media.co/a-second-tea-breach-reveals-users-dms-about-abortions-and-cheating/.

[64] *See*, *e.g.,* David Lang, Benjamin Listyg, Brennah V. Ross, Anna V. Musquera, and Zeve Sanderson, *Do Age-Verification Bills Change Search Behavior? A Pre-Registered Synthetic Control Multiverse,* OSF (Mar. 2025), https://osf.io/z83ev; Dominic Preston, *The VPN Panic Is Only Getting Started*, Verge (Nov. 27, 2025),

Entities engaged in age verification should be required to delete underlying proof of age data, such as biometric scans or images of government ID, after the verifier determines the user's age or age range. Data that is present on proof of age documents, such as place of birth, date of birth, and more, are sensitive and difficult or impossible to change; prolonged retention of age-related data or ID-data makes users vulnerable to identity theft and misuse of their personal data. There is no legitimate reason for age verification providers to retain this data after age determination, given its sensitivity. It also opens up companies as targets of malicious attacks by actors seeking to access sensitive data for profit or abuse. The impact of data breaches can be profound, forcing victims to shut down or secure bank accounts, freeze their credit at the three big agencies, or acquire new IDs to thwart or rectify identity theft. Deleting underlying age proof data immediately after verifying age can help verifiers minimize data breaches and inappropriate access to data, all while better protecting users. Some age verification providers have promised to delete underlying proof of age data (such as a face scan) seven days after collecting it to comply with some laws.[65] But Georgia Tech's forthcoming research indicates the picture may be more complicated than this depending on differing requirements around the world, and there's no guarantee every service will delete data they acquire quickly unless they are obligated to do so.[66] Further, proving companies' compliance with deletion requirements is very difficult for government enforcers from the outside, which makes whistleblower protections much more important. Verifiers and policymakers should prefer tokenized age proof systems when available, so that they never receive the underlying documentation, just an attested proof of age.

Services required to conduct age verification should also be required to provide users clear transparency and disclosure on the method used, what data is collected and stored, and with whom data is shared. Furthermore, users should know who is operating the age assurance system and how to

---

https://www.theverge.com/tech/827435/uk-vpn-restrictions-ban-online-safety-act; Bryan Schott, *Utahns Search for VPNs After Pornhub Blocks Adult Content from the Beehive State*, Salt Lake Trib. (May 3, 2023) https://www.sltrib.com/news/politics/2023/05/03/utahns-search-vpns-after-pornhub/.

[65] *See, e.g.*, Emma Roth, *Ready or Not, Age Verification Is Rolling Out Across the Internet*, Verge (Jul. 30, 2025), https://www.theverge.com/analysis/715767/online-age-verification-not-ready; Jon Brodkin, *Reddit's UK Users Must Now Prove They're 18 to View Adult Content*, Ars Technica (Jul. 14, 2025), https://arstechnica.com/tech-policy/2025/07/reddit-starts-verifying-ages-of-uk-users-to-comply-with-child-safety-law/.

[66] *See* Shreyas Minocha, *et al*., *supra* note 37.

meaningfully request deletion of data and remedy inaccurate age classification if and when it occurs. This includes instances where users have already opted into age assurance but change their mind at a later point and seek to delete their account and the data that was used to verify or assign them an age.

These criteria match or overlap to some degree with principles set by international regulators in Europe and beyond. In addition to the forthcoming research mentioned above from Georgia Tech, other investigations are revealing popular age assurance providers who are not meeting commitments to privacy set by regulators. For example, an evaluation by AI Forensics of France's AgeGO, an age verification provider gating youth access to adult content, found that the provider did not adequately mitigate risks to user privacy or meet accuracy, transparency, and other set criteria by ARCOM, France's independent administrative agency.[67]

Each of the bills before this Committee that incentivizes or requires platforms to determine the age of all of their users in order to sort out which of them are minors should include the above principles. By holding age verification providers and services that conduct age verification to these rights-respecting criteria, Congress can minimize the degree to which deployments of age verification undermine user rights.

## IV. Creating good policy requires taking into account the varied perspectives and experiences of minors and their caregivers.

Minors and their caregivers have strategies for and opinions about managing minors' online lives. These strategies and opinions are informed by lived experience that undoubtedly could improve policymaking by legislators and companies related to minors' online activities. CDT has conducted research where we asked a sample of teens and their parents about features proposed in current child safety proposals, including some that are being considered by the Committee today.[68] What we found can help improve discussions around kids' safety.

---

[67] Paul Bouchaud, *Technical Report: AgeGO Age Verification on Pornographic Platforms*, AI Forensics (Sept. 2025), https://aiforensics.org/uploads/AIF_report_AgeGO_porn_platforms.pdf.

[68] Michal Luria & Aliya Bhatia, *What Kids and Parents Want: Policy Insights for Social Media Safety Features*, Ctr. for Democracy & Tech. (2025), https://cdt.org/insights/what-kids-and-parents-want-policy-insights-for-social-media-safety-features/.

- Age assurance: Parents and teens expressed significant safety and privacy concerns with subjecting minors to age assurance methods. They viewed ID-based and face scanning methods as particularly invasive and expressed skepticism of their efficacy. Participants favored parent-centered approaches that enabled parents to declare their children's age and consent to which apps their children downloaded.
- Algorithmic Feed Controls: Teens prefer feeds that provide algorithmic recommendations, and trust algorithmic recommendations to provide interesting, diverse and appropriate content. Their trust is made possible precisely because they feel that they are in control of that content. They prefer lightweight controls such as "not interested" functions and swiping quickly to display disinterest, over more invasive functions like pop-ups.
- Screen Time: Parents and teens appreciated reminders of time spent and parent-led limits on screen time, but they did not favor app-based, content-based, or third-party enforced limits. Strict curfews were viewed as draconian and, potentially, counterproductive.
- Parental Access and Control: Teen participants were generally accepting of parental visibility into their activities, but strongly opposed parental ability to delete content or apps without their consent. Parents broadly agreed, preferring to engage in high-level approval of app downloads and other significant actions, while viewing controls over every day approvals, like joining a group chat or adding a contact, as excessive and unnecessary.

A number of the bills before the Committee today would require the government to conduct studies that lead to best practices for children's safety online. CDT supports that evidence-based approach. The Kids Internet Safety Partnership Act[69] explicitly requires the Partnership to coordinate with parents and minors, as well as other stakeholders, to identify the risks and benefits for minors with respect to the use of websites, online services, and mobile applications and widely accepted or evidence based best practices for minors of different ages. This kind of inclusive consultation in the

[69] H.R. ___, Kids Internet Safety Partnership Act (119th Cong. 1st Sess.), https://docs.house.gov/meetings/IF/IF17/20251202/118714/BILLS-119pih-HR___KidsInternetSafetyPartnershipActRepFry.pdf.

development of policy will ensure better outcomes for everyone. Moreover, careful and holistic approaches that study complex issues and draw in multiple perspectives allow a fuller consideration of the potential interventions all stakeholders can implement. Some interventions, when required by the government, are unwise or otherwise legally difficult to implement, but when voluntarily implemented in particular contexts by industry, civil society, technologists, families, or other actors in the online ecosystem can improve online safety and freedom for minors and adults alike.

A study approach might help build nuance into company and legislative children's safety policy in other ways, and could help fill in research gaps. Many proposals before the Committee today and many company policies recognize that it is impractical and inappropriate to treat all minors the same as they age. This was also a reality reflected by the parents and teens who participated in CDT's recent study.[70] What's appropriate for children under 13 will not be the same as what's appropriate for a 16 year old. The content that is appropriate for those age groups will be different and the level of independence those age groups should have in conducting their online lives should also, likely, be different.

Recently, some services have begun to filter and display content differently to teen and minor users.[71] This task is not without its complications, in part, because content moderation systems themselves are complicated, generally employing a combination of human moderators, automated recommendations, user reporting tools, and community guidelines to determine what content to display to whom and when. Researchers have noted the difficulty in determining what content is "age appropriate."[72] For example, some minors exhibit greater maturity at an earlier age, indicating a readiness for more adult content, while others take more time to reach certain stages of readiness. Moreover, different communities define what content is "age appropriate" differently, adding another

[70] Luria & Bhatia, *supra* note 68.
[71] *See, e.g., About Instagram Teen Accounts*, Instagram (last visited Nov. 27, 2025), https://help.instagram.com/995996839195964; *Supervised Experiences for Teens*, YouTube (last visited Nov. 27, 2025), https://support.google.com/youtube/answer/15253498; *Safeguards for Teens*, SnapChat (last visited Nov. 27, 2025), https://parents.snapchat.com/safeguards-for-teens.
[72] Michal Luria & Aliya Bhatia, *The Kids Are Online: Research-Driven Insights on Child Safety Policy,* at 17, Ctr. for Democracy & Tech. (Feb. 2025), https://cdt.org/wp-content/uploads/2025/02/2025-02-14-Child-Safety-Symposium-Summary-report-final.pdf.

layer of complexity.[73] Finally, some filtering for age appropriateness can limit minors' access to beneficial and educational content. Over-filtering can — and has — led to the reduction in the display of appropriate LGBTQ+ content, for example.[74] Further study would be helpful to understand how to define what content is age-appropriate and how to build flexibility into that definition depending on relevant factors. In requiring further study, Congress might also consider ways to assist researchers in conducting further study of issues related to kids' activities online.[75]

## V. Congress must not unduly restrict states' ability to act – and, in particular, must reject any false deal that conditions kids' online safety on preempting states' ability to regulate AI.

States have long played a critical role in protecting against harms to children. State level protections specifically applicable to children online run the gamut from restrictions on access to social media platforms or constitutional content (laws that raise significant constitutional concerns), to the creation of educational programs to help children learn to navigate the online world, to meaningful privacy protections that mitigate the monetization of children's online activities.[76] Generally applicable laws also provide significant protections for children. These laws might include state unfair and deceptive trade practices statutes, tort and common law claims, civil rights statutes, educational protections, criminal laws, and comprehensive privacy statutes that contain heightened standards for children's data. Congress should be very careful when seeking to displace that authority and these existing laws.

As noted earlier, H.R. 6291, COPPA 2.0, H.R. ___, KOSA, and many of the other bills at issue today would preempt "any law, rule, regulation, requirement, standard, or other provision having the force and effect of law that *relates to* the provisions of this Act." We are concerned that this standard

[73] *Id*.
[74] *See, e.g.*, Brooke Tanner & Nicol Turner Lee, *Children's Online Safety Laws Are Failing LGBTQ+ Youth*, Brookings Inst. (Jul. 9, 2025), https://www.brookings.edu/articles/childrens-online-safety-laws-are-failing-lgbtq-youth/; Taylor Lorenz, *Instagram Blocked Teens from Searching LGBTQ-Related Content for Months*, User Mag (Jan. 6, 2025), https://www.usermag.co/p/instagram-blocked-teens-from-searching.
[75] Luria & Bhatia, *supra* note 72.
[76] *See, e.g.*, *Social Media and Children 2025 Legislation*, National Conference of State Legislatures (last updated Oct. 24, 2025), https://www.ncsl.org/technology-and-communication/social-media-and-children-2025-legislation.

will sweep very broadly to preempt much of the legislation that either specifically protects children or provides significant protections to children online, even if the bills at issue today do not specifically cover the activities addressed by the state law or the state law provides better protections for children. In general, in legislation that provides protections to children, Congress has chosen to narrowly preempt, if it chose to preempt at all, state level efforts. The preemption standard contained in many of the bills before the Committee represents a problematic break with that precedent that could undermine protections in place for children across the country.

Preemption of state laws is always a fact-specific analysis. Generally, however, the scope of preemption in any given proposal should correspond to the strength and scope of the protections being enacted. APRA, for example, was a comprehensive consumer privacy proposal, justifying the preemption of state comprehensive privacy laws, but APRA also exempted certain categories of laws from the scope of their preemption clauses, including consumer protection laws of general applicability, employee privacy laws, student privacy laws, and data breach notification statutes.[77] These exemptions rightly sought to preserve longstanding consumer, employee, and student protections and to avoid unintended consequences.

The proposed preemption of state laws under APRA and ADDPA also represented what was, in the view of its authors and supporters, a fair trade-off. Congress would put in place needed protections that would apply nationwide (instead of only in a specific state) and corresponding state level protections would be preempted. But the legislation currently under consideration today, even taken together, would not justify broader preemption of generally applicable laws as they relate to children, nor would it justify the preemption of other state level protections specifically applicable to children. It would be both ironic and harmful if Congress's passage of laws intended to protect children online ended up leaving them with *fewer* protections.

To make matters worse, public reporting indicates that Congress may be negotiating a deal to pass a kids' safety package that includes the extremely controversial provision preempting state laws

[77] American Privacy Rights Act, H.R. 8818 (118th Cong., 2d session), https://www.congress.gov/bill/118th-congress/house-bill/8818/text.

on artificial intelligence.[78] That would be wholly unjustified. Many of the bills under consideration today do not meaningfully address emerging technologies like generative AI. To the extent that the bills before the Committee today do address rapidly emerging AI technologies, they do not do so in a comprehensive fashion as applied to children. And, of course, these bills do nothing to provide guardrails or protections with respect to the many various ways in which the use of AI increasingly impacts everyone in this country, including as to consequential decisions relating to their employment, finances, education, and health. Bipartisan state legislators,[79] Attorneys General,[80] and Governors,[81] as well as a broad coalition of civil society organizations, including child safety advocates,[82] have all come out in opposition of such a moratorium. Companies should not get a free pass for committing fraud or illegal discrimination just because they use AI to do it. Passing any type of broad preemption, including a broad moratorium, on states' ability to enact laws related to AI without putting in place strong federal protections commensurate with the scope of any such preemption would create a situation in which lawmakers at all levels were unable to enact laws to address harms and risks as AI rapidly evolves and spreads throughout our economy and society.[83]

---

[78] Ruth Reader & Carmen Paun, *A Plan to Merge Kids' Safety with Preempting State AI Laws*, Politico (Nov. 26, 2025), https://www.politico.com/newsletters/future-pulse/2025/11/26/a-plan-to-merge-kids-safety-with-preempting-state-ai-laws-00668767.

[79] Letter from Brandon Guffey & Liz Larson, *et al*., to U.S. House of Representatives and U.S. Senate, *NDAA State Policymaker Coalition Letter - Oppose AI Preemption* (Nov. 24, 2025), https://ari.us/wp-content/uploads/2025/11/NDAA-State-Policymaker-Coalition-Letter-11-23-25-Oppose-AI-Preemption.pdf.

[80] Letter from National Association of Attorneys General to House Speaker Mike Johnson and House Minority Leader Hakeem Jeffries and Senate Majority Leader John Thune and Senator Minority Leader Chuck Schumer, *State Attorneys General Urge Congress to Preserve Local Authority on AI Regulation* (Nov. 25, 2025), https://www.naag.org/policy-letter/state-attorneys-general-urge-congress-to-preserve-local-authority-on-ai-regulation/.

[81] Letter from Gov. Sarah Huckabee Sanders, *et al*., to Senate Majority Leader John Thune and House Speaker Mike Johnson, *Joint Governors Letter on One, Big, Beautiful Bill AI Moratorium* (Jun. 27, 2025). https://governor.arkansas.gov/joint-governors-letter-on-one-big-beautiful-bill-ai-moratorium/.

[82] Letter from Coalition of Civil Society Organizations to Senate Majority Leader John Thune *et al*. (Nov. 24, 2025), https://cdt.org/wp-content/uploads/2025/11/Letter-Opposing-AI-State-Preemption-November-19.pdf.

[83] Travis Hall, *Throw the AI Regulations Ban out with the Byrd Bath Water*, Ctr. for Democracy & Tech. (May 20, 2025), https://cdt.org/insights/throw-the-ai-regulations-ban-out-with-the-byrd-bath-water/.

## Conclusion

The Committee is right to express concern about the impact of emerging technologies on children. The wide range of proposals currently before the Committee contain valuable ideas, including ones to increase the evidence base through which parents and young people can make decisions about and increase control over their experiences online. Some also raise constitutional and practical concerns about young people's access to lawful content, or the ability of adult users to access information privately and freely online. For these reasons, we urge the Committee to proceed with judgment and prioritize solutions that protect children's safety while also valuing privacy and free expression rights.

Legislative proposals that would enact meaningful data minimization restrictions and other data privacy protections either for everyone or, at a minimum, beginning with enhancing protections for children would help to address some of the root causes of many of the concerns for kids' safety online. We look forward to working with the Committee members and staff to enact meaningful protections for children and for everyone online.