

To: House Committee on Energy & Commerce Privacy Working Group
From: Common Sense Media
Subject: Feb. 21, 2025 Request for Information
Date: April 7, 2025

Common Sense Media is dedicated to helping kids and families thrive in a rapidly changing digital world, and advocates to improve young people's experiences with technology. Since launching in 2003, Common Sense has helped millions of families and kids think critically and make smart choices about the media they create and consume, offering age-appropriate family media ratings and reviews, a digital citizenship curriculum for schools, and research reports that fuel discussions of how media and tech impact kids today. It is through these tools that our work reaches over 150 million users worldwide and 1.4 million educators every year across the country. Common Sense also educates legislators and regulators around the globe about children's unique vulnerabilities online. Common Sense has successfully sponsored and supported privacy legislation around the country, including landmark consumer and student privacy laws like the California Consumer Privacy Act (2018) and Student Online Personal Information Protection Act (2014). In 2024, Common Sense supported, among other laws, the Maryland Online Data Privacy Act and the New York Child Data Protection Act.

Common Sense believes that everyone deserves strong privacy protections. These protections involve ensuring laws hold all responsible parties accountable, and that rules protect personal information broadly and require not just transparency but data minimization and clear prohibitions on practices like targeted ads. Laws must accommodate future changes in technology, and do not need to – but can constitutionally – use age assurance when needed. In addition, laws should not inhibit states' rights to innovate. And lastly, laws are only meaningful when they come with effective enforcement. Children and teenagers are especially vulnerable to privacy risks and harms and deserve the utmost protections.

Privacy Risks are Rampant and Youth are Especially Vulnerable Online

Privacy risks are rampant on social media and other platforms. Tracking and targeting minors is very common—even in circumstances when laws purport to restrict it. One study found ad tech companies have gathered at least 72 million data points on children by the age of 13 (precisely when the current Children's Online Privacy Protection Act (COPPA) is supposed to limit collection).¹ Documents exposed in litigation show that social media companies collect reams of information on youth—including classifying objects and people in images and videos shared – and uses this to target youth with products, eke more money out of advertisers, and find the “exact”

¹ Katie Joseff, *Behavioral Advertising Harms: Kids and Teens* (2022), https://www.common sense media.org/sites/default/files/featured-content/files/behavioral_-surveillance-advertising-brief.pdf

mix of materials to make it hard for youth to turn away from digitally addictive products.² Children and teens are online a lot – Common Sense research found children under 8 spend 2.5 hours a day with screen media, and by age 4 more than half have their own devices.³ Meanwhile, tweens and teens spend over 5.5 and 8.5 hours a day on screens (in addition to school work).⁴ According to the U.S. Surgeon General’s 2023 Advisory on Social Media and Youth Mental Health, 8th and 10th graders spent an average of 3.5 hours a day on social media, as of 2021.⁵ Whenever young people are using their devices—watching videos, chatting with friends, or gaming—information is collected. And mountains more data is collected on youth in school—simply as part of students’ efforts to get an education. Children simply trying to learn can unknowingly have their information shared with advertisers and tech giants seeking to profit off of such insights.⁶

Youth are susceptible to privacy harms because of their extensive interaction with digital technology. They are also particularly susceptible to privacy harms because of their unique developmental needs. For example, minors’ executive functioning skills, which are critical to directing attention and behavior, are still developing throughout childhood and adolescence.⁷ Young children do not understand the consequences of information shared with apps and platforms. They believe, for example, that deleting an app or information within an app will delete it from the internet, and they do not expect or understand that a game they play may gather

² See, e.g., Complaint at 77-78, 82, 157, *Commonwealth v. TikTok Inc.*, No. 2484CV2638-BLS (Mass. Super. Ct. Feb. 3, 2025), available at <https://www.mass.gov/doc/tiktok-complaint-unredacted/download>. TikTok’s privacy policy states it collects: “User-generated content, including comments, photographs, livestreams, audio recordings, videos, text, hashtags, and virtual item videos that [the user] choose[s] to create with or upload to the Platform (“User Content”) and the associated metadata, such as when, where, and by whom the content was created”), “Information [the user] share[s] through surveys or [their] participation in challenges, research, promotions, marketing campaigns, events, or contests such as [their] gender, age, likeness, and preferences.” TikTok’s policy states it also “automatically collects certain information” from users when they use its platform: “including internet or other network activity information such as [a user’s] IP address, geolocation-related data, unique device identifiers, browsing and search history (including content [a user] ha[s] viewed in the Platform), and Cookies” ... ““Image and Audio Information,” i.e., “information about the videos, images and audio that are a part of your User Content, such as identifying the objects and scenery that appear, the existence and location within an image of face and body features and attributes, the nature of the audio, and the text of the words spoken in your User Content” which TikTok uses “for demographic classification, [and] for content and ad recommendations.”

³ Common Sense Media, *The Common Sense Census: Media Use by Kids Zero to Eight* 1, 4 (2025), <https://www.common Sense Media.org/sites/default/files/research/report/2025-common-sense-census-web-2.pdf>.

⁴ Common Sense Media, *The Common Sense Census: Media Use by Tweens and Teens* 3 (2021), https://www.common Sense Media.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf.

⁵ U.S. Surgeon General, *Social Media and Youth Mental Health* 6-7 (2023), <https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf>.

⁶ Press Release, Fed. Trade Comm’n, *FTC Says Ed Tech Provider Edmodo Unlawfully Used Children’s Personal Information for Advertising and Outsourced Compliance to School Districts* (May 22, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ed-tech-provider-edmodo-unlawfully-used-childrens-personal-information-advertising>.

⁷ Heather J. Ferguson et al., *The Developmental Trajectories of Executive Function from Adolescence to Old Age*, *Sci. Rep.* (2021), <https://www.nature.com/articles/s41598-020-80866-1.pdf>.

information about them from external sources.⁸ Further, adolescence is a period of heightened reward-seeking behavior as a result of increased brain activity related to dopamine.⁹ This contributes to teens' tendency to seek out reward stimuli,¹⁰ such as those offered by social media and gaming platforms. Social acceptance also activates the reward center in adolescent brains,¹¹ rendering youth susceptible to the social manipulation and peer pressure applied by design features intended to maximize user engagement. It is critical to consider these and other unique aspects of minors' development when assessing the business practices and design techniques that companies use to attract young users' time and attention.

When information is collected from children, teens, and all users, it can be used to label and limit, and put individuals into ad categories. These categories can be based on their preferences and interests, purchases, and even state of mind. A leaked Meta (then Facebook) memo told advertisers it could identify when teenagers felt worthless, stressed, or insecure.¹² In 2019, Meta categorized almost three-quarters of a million kids under 18 as interested in gambling, and almost a million as interested in alcoholic beverages.¹³ Whether or not social media companies actually push alcohol or gambling on these minors, they can profit from it by advertising games with gambling elements or other features that would be particularly appealing to such users.

AI technology multiplies privacy risks, as companies seem eager to collect ever more data for "training".¹⁴ AI technology is especially concerning given its novelty, the speed and autonomy at which the technology can operate, and the frequent opacity even to developers of AI systems about how inputs and outputs may be used or exposed. Particularly problematic uses of AI in products used in education and/or by children so far include products that use emotion detection, biometric data, facial recognition (built from scraping online images that include children), AI companions, automated education decisions, and social scoring. This list will continue to grow as AI is further adopted.

⁸ Kaiwen Sun et. al., "They See You're a Girl if You Pick a Pink Robot with a Skirt": How Children Conceptualize Data Processing and Digital Privacy Risks, 2021 ACM CHI Conference on Human Factors in Computing Systems 1, 6-7 (2021), <https://doi.org/10.1145/3411764.3445333>.

⁹ Eveline A. Crone, *Executive Functions in Adolescence: Inferences from Brain and Behavior*, 12 Developmental Science 825, 829 (2009); Adriana Galvan, *Adolescent Development of the Reward System*, 4 Frontiers Hum. Neuroscience 1, 1 (2010).

¹⁰ Ashley C. Parr et al., *Dopamine-Related Striatal Neurophysiology Is Associated with Specialization of Frontostriatal Reward Circuitry Through Adolescence*, 201 Progress in Neurobiology 1, 1 (2021); Dustin Albert & Laurence Steinberg, *Judgment and Decision Making in Adolescence*, 21 J. Res. on Adolescence 211, 217-219 (2011).

¹¹ Zara Abrams, *Why Young Brains Are Especially Vulnerable to Social Media*, American Psychological Association (Feb. 3, 2022), <https://www.apa.org/news/apa/2022/social-media-children-teens>.

¹² Katie Joseff, *Behavioral Advertising Harms: Kids and Teens 4* (2022), https://www.common sense media.org/sites/default/files/featured-content/files/behavioral_advertising-brief.pdf.

¹³ *Id.* at 4.

¹⁴ See, e.g., Shira Ovide, *Alexa is Getting Creepier. Take This One Step to Improve Your Privacy.*, Wash. Post (Mar. 18, 2025), <https://www.washingtonpost.com/technology/2025/03/18/amazon-alexa-privacy-voice-recordings/?>.

All Digital Players Have Responsibilities to Protect Privacy (“Roles and Responsibilities”)

All entities that collect, use, store, share, or benefit and profit from data collection bear a responsibility to ensure individuals’ privacy is protected. Many laws allocate responsibilities between those controlling data processing activities (the “controller” in laws like VA, or “business” in CCPA) and those doing the actual processing (the “processor” or “service provider”). These distinctions, coupled with contractual requirements between entities, make sense.

In addition, while laws may take into consideration what is “reasonable” (such as “reasonable security measures”) based on the size or capacity of a business, small size alone should not absolve entities of responsibility. Indeed, in the youth space, many start ups with limited resources can still pose huge risks to children’s data. It is often these smaller companies that do not even have a trust and safety or privacy team that pose the greatest risk to young user’s data. For example, last year, the [NGL app](#) was engaging in privacy violations and unfair business practices that hurt children and teens. Small anonymous peer messaging apps can quickly appear on the scene, attract young users, and then go defunct—with youth left unprotected. Anecdotal, small AI chatbots are also a growing concern. Thus, laws should not provide blanket exemptions for small companies. Rather, a law should look to both size and what an entity actually does, including its business model. Many state laws consider this, for example, applying if entities *either* process data of a certain number of consumers, or hit a certain revenue threshold, or derive a certain percentage of revenue based on the sale of data.

Rules Must Broadly Protect The Privacy and Security of Personal Information, Including in An AI Era (“Personal Information, Transparency, Consumer Rights”, “Data Security”, “Artificial Intelligence”)

Personal Information Should Be Broadly Protected

Personal information protected by a law should include any data that is linked or reasonably linkable to an identified or identifiable individual or device (if that device identifies or is linked or reasonably linkable to an individual). This is a standard seen in multiple laws like California and Oregon. Personal information may be collected directly from an individual, or indirectly (such as personal information input about a student by a teacher), or derived by a company (consumer profiles on social media).

While personal information should be broadly protected—and modern consumer privacy laws do define it broadly, whether or not they offer adequate protections—many laws separately distinguish sensitive personal information (such as about health, or religious beliefs, or biometrics, or a minor’s information, or precise geolocation, or government identifiers). Historically, sensitive information could carry additional risk if disclosed. Modern laws and models also consider data collected surreptitiously about consumers—such as online activities—to be sensitive information. [Insert site, also EPIC model, Washington Privacy law] While the distinction between sensitive and non-sensitive information can be useful, it is increasingly possible to determine very sensitive

things about consumers from seemingly benign information (such as pregnancy status from moisturizer purchases (cite Target), and therefore it bears considering whether sensitive data still is still a meaningful category. This question is particularly relevant in the AI era, when information from individuals may be input into generative AI and used to train generative AI models. To the extent it is, it should encompass sensitive inferences even from innocuous data, and data about sensitive populations, like children and teens.

Transparency is Necessary But Not Sufficient to Protect Privacy

Disclosures and transparency about use of personal information are necessary, but in no way sufficient, and privacy law should not rely on the fiction of “notice and choice” because there was a disclosure and an ostensibly informed choice to use a service.

First, consumers—especially youth, and especially students—do not have a real choice in using many services, and many consumers do not understand privacy notices as they are drafted. While it is critical that information be provided in detailed notices for researchers and regulators, it is also important that information be clear and accessible to parents and kids. Information should be presented to them at relevant points in time in digestible formats. Parents and teens today seeking information often find themselves adrift in a sea of lengthy notices and legalese, causing many to simply give up with resignation. Parents and other caregivers are too busy and in many cases too unfamiliar with technology to know, or have the time to know, which features to turn on or off and how to turn them on or off.

Second, many privacy notices may in and of themselves be misleading.¹⁵ And, confoundingly, the misleading aspects can be compounded by efforts to streamline notices. For example, to provide more clarity and accessibility of a product’s privacy practices, some companies have published separate “privacy principles” or “privacy center” webpages to help summarize their privacy practices, but often these privacy summary websites do not actually disclose any of the “worse” privacy practices they engage in with children, teens, or adults’ data.¹⁶ This can create a false sense of safety for children and parents who believe these products are more privacy protecting than they actually are because not all the most important facts are included. In addition, recent moves to app store privacy and data safety labels –while purporting to improve clarity and accessibility of privacy – have been found to show that these labels, which may be self reported and unvalidated by platforms, claim safer privacy practices than what their privacy policies state.¹⁷ Upwards of 60% of popular apps used by children and teens in both App Stores have been found to display

¹⁵ Common Sense Media, *2023 State of Kids’ Privacy* 20 (2023), https://www.common Sense Media.org/sites/default/files/research/report/common-sense-media-2023-state-of-kids-privacy_0.pdf

¹⁶ See Microsoft Privacy Principles, <https://privacy.microsoft.com/en-US> (last visited Apr. 7, 2025) (“Microsoft’s privacy center does not disclose its “worse” privacy practices of selling data, displaying targeted advertisements, or tracking users across the internet and over time for commercial purposes.”)

¹⁷ Anne Stopper & Jen Caltrider, *No Evil: Loopholes in Google’s Data Safety Labels Keep Companies in the Clear and Consumers in the Dark*, 5, 14 (2023), https://assets.mofoprod.net/network/documents/PNI_Google_Play_Store_Research_Report_2023.pdf.

false privacy information to parents and children, completely negating trust and any shared clarity or accessibility of a product's privacy practices.¹⁸

Ultimately, while transparency is essential, it is not sufficient to protect young users online. Instead, laws must require companies to adopt principles of data minimization, ban targeted ads to youth, and demonstrate a “duty of care” for all users and especially children and teens.

Data Minimization and Prohibiting Targeted Ads to Youth are Among Key Provisions

A privacy law should enable individuals to have access, deletion, correction, and transparency rights. But most importantly, it should require data minimization from the outset, and it should prohibit the sale of data for children and teens, and any data deemed sensitive. Common Sense points to the recent Maryland Privacy Bill, and to proposed bipartisan COPPA 2.0, as two good examples of strong privacy protections for consumers and youth. Common Sense is also a supporter of the model privacy bill by EPIC and Consumer Reports which contains critical elements.¹⁹

Data minimization is vitally important. Data minimization is a requirement for businesses at the outset to limit what they collect to what is reasonably necessary, and what consumers reasonably expect based on their interactions with the businesses. Data minimization does not require consumers to take numerous steps –or any steps–to stop unnecessary personal information collection. This is important, because research shows defaults are very sticky. Data minimization also prevents companies from claiming they had consent to collect, use, process, or share data in unexpected ways because it was buried in a lengthy policy. Consistent with data minimization, there should be clear prohibitions on selling or using children and teens' information for targeted ads, in addition to any other information deemed sensitive. A child's data should not be sold or shared. Targeted advertising should be banned for youth under 18. This is especially important because children are often sharing information in educational contexts, where educators and/or parents may have little insight into digital products and little ability to say no.

Holding less data inherently means there's less to protect (and less to lose) which strengthens consumer safety by design. These safeguards are particularly vital for protecting the data of children and teens, who are increasingly harmed by data breaches. A 2024 report found that one in eight children in the US had their data exposed in a breach and one in 19 US children had been affected by identity theft and fraud in the previous six years – with those age 6 and under and teens at the greatest risk.²⁰

¹⁸ Yucheng Li et. al., *Understanding iOS Privacy Nutrition Labels: An Exploratory Large-Scale Analysis of App Store Data*, 2022 CHI Conference on Human Factors in Computing Systems Extended Abstracts 1 (2022), <https://doi.org/10.1145/3491101.3519739>.

¹⁹ Electronic Privacy Information Center (EPIC), *The State Data Privacy Act* (2025), <https://epic.org/wp-content/uploads/2025/04/State-Data-Privacy-Act-EPIC-CR-April2025.pdf>

²⁰ Tracy Kitten, 2024 Child & Family Cybersecurity Study (2024), <https://landing.escalent.co/hubfs/24-5014J-CS-2024%20Child%20&%20Family%20Cybersecurity%20Study.pdf>.

Data minimization along with the additional protections outlined above will significantly reduce the volume of personal data collected and retained by businesses. This not only limits the exposure of sensitive data in the event of a breach, but also reduces the overall number of vulnerabilities. By limiting the collection and retention of personal data, we can reduce these risks and foster a digital environment that prioritizes user privacy and security from the outset. At the same time, these protections disrupt the data broker and targeted advertising ecosystem by curbing the widespread sale and purchase of data that fuels surveillance advertising systems, further reducing the incentives for companies to stockpile excessive amounts of user data.

In addition, a law could promote thoughtful privacy and security by design. By proactively addressing risks in the product development stage, and undergoing regular audits and providing patch updates, companies can get ahead of issues and from the start create healthier, more privacy protective products for youth.

Any Law Must Accommodate For Future Technology

Lastly, a law should be flexible enough to address AI and future technologies. As the federal government further details the impacts associated with AI use, common uses of AI by kids should be evaluated through a risk based analysis and designated or managed as high risk. Privacy protections in such high risk settings should by default be high. Data minimization should be addressed and considered in the AI space. Privacy and security by design, audits, transparency, or enforcement) to prevent or address potential harm. Privacy law should explicitly address use (especially for training) and sharing of personal information (PI) by AI tools. State proposals are considering this. For example, updates to student privacy laws that would limit use of PI for training only if in furtherance of a K-12 school purpose and for the use and benefit of that school.²¹ In the consumer space, there are proposals to generally prohibiting the use of children's PI for training AI models, unless deidentified or aggregated and with consent.²² Rulemaking by expert agencies can help ensure privacy laws keep up to date with evolving technology.

Age Assurance Need Not, But Can, Be a Part of Privacy Law

Whenever there are discussions of special protections for children and teens, the question of how to identify such children and teens occurs. Common Sense believes that the vast majority of companies profiting off of children and teens' information already know they are dealing with children and teens, and therefore, such questions are overblown. However, Common Sense also believes it is constitutionally possible to use proportional, privacy-protective age assurance to

²¹Assem. B. 1159, 2025–2026 Leg., Reg. Sess. (Cal. 2025), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260AB1159.

²² Assem. B. 1064, 2025–2026 Leg., Reg. Sess. (Cal. 2025), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260AB1064; Common Sense Media, LEAD on AI Act Fact Sheet (2025), <https://www.common sense media.org/sites/default/files/featured-content/files/lead-on-ai-fact-sheet.pdf>

ensure protections for children and teens. Rapidly advancing technology makes this so. For further background on this related topic, Common Sense attaches as supplemental material its white paper, *US Age Assurance is Beginning to Come of Age*.²³

Any Federal Law Should Not Inhibit States' Rights to Innovate ("Existing Privacy Frameworks & Protections")

A federal privacy law should be a floor, not a ceiling, akin to what many federal consumer protection laws offer. Technology is advancing at a rapid pace, and states have been responding to its advances. Congress is slower to act. (COPPA, for example, is over 25 years old, and despite its updates passing out of the Senate with almost universal support last year it has still not been updated). Given the likelihood of future changes in technology and company practices, it is highly likely that legislators will need to respond to these changes with new legislation. We have seen that states are much more likely to iterate and respond on a more timely basis.

In addition, existing sectoral laws may be more appropriate to address specific issues at hand. For example, in the education context or the healthcare context, laws may be best tailor-fit to the context. However, sectoral laws require consideration on a case by case basis, as some sectoral laws (such as in the financial sector) seem weak and out of date compared to more modern comprehensive consumer proposals. When there are carve outs for sectoral laws, those carve outs should only be for laws that are more privacy protective and only for specific data governed by another law. It does not make sense to carve out, for example, all "HIPAA entities"--for example, many large tech companies have services governed by HIPAA and the entity as a whole should not have a blanket exemption from consumer privacy laws just because of that.

Laws are Only as Strong as Their Enforcement ("Accountability & Enforcement")

Legislation is only as strong as its enforcement. Common Sense believes that strong enforcement can occur in a variety of ways, but primarily it occurs through well-funded expert enforcers and through private litigation. Common Sense supports a fully staffed Federal Trade Commission. It supports enforcement by that Commission and by state Attorney Generals and state expert agencies like the California Privacy Protection Agency. Common Sense also believes there is a place for private rights of actions, so consumers can take appropriate redress for harms that befall them or their children. To the extent Congress is interested in safe harbors, Common Sense believes such safe harbors need to be transparent and accountable. Otherwise, they will have little incentive to require their clients to protect privacy.

Companies will not act to comply with the law if they do not believe there will be any repercussions. And we have seen that companies will not willingly take on privacy protective actions on their own. For existing laws to have any real impact, and inform federal policy, we need

²³ Common Sense Media, *U.S. Age Assurance Is Beginning to Come of Age* (2024), https://www.commonsensemedia.org/sites/default/files/featured-content/files/2024-us-age-assurance-white-paper_final.pdf

to start holding companies accountable when they don't comply. Otherwise, the industry will continue making money by influencing and exploiting kids and families' data for commercial purposes, all while claiming they respect our privacy.

Questions? Please contact Ariel Fox Johnson, Senior Advisor on Privacy, afoxjohnson@commonsense.org