PUBLIC KNOWLEDGE

THE KIDS AREN'T ALRIGHT ONLINE: HOW TO BUILD A SAFER, BETTER INTERNET FOR EVERYONE

2025 | AUGUST

SARA COLLINS
MORGAN WILSMANN

The Kids Aren't Alright Online: How To Build a Safer, Better Internet for Everyone

Sara Collins
Morgan Wilsmann

Acknowledgements

At Public Knowledge, we believe that any laws that aim to minimize online harms should be made available to *all* users, not just child users. However, state and federal legislators seem determined to write child-specific legislation only. If such is the case, then we must present a vision for policymakers that centers the needs of children and teens, keeps the internet accessible for adults (without having to give up even more private data), and actually addresses the tangible harms facing youth users.

This paper aims to provide that vision. We would not have been able to write it, however, without first consulting other civil society organizations, industry leaders, and academics. In January of 2025, we convened representatives of these diverse stakeholder groups in an off-the-record Public Knowledge Policy Konclave workshop to engage in dialogue and debate on how to construct such a vision. Make no mistake – this proposal is not meant to be a documentation of consensus; rather, an attempt to create policy that addresses the failings of the internet while also preserving its overwhelming benefits. All participants in the Public Knowledge Policy Konclave contributed and shared their ideas with the assurance that this paper will reflect the learnings and positions of only Public Knowledge. We are grateful for their participation in sharpening our understanding and positions.

A special acknowledgement to Michelle Richardson, who acted as our rapporteur for this project and generously shared her insights on our data collection. Her contributions proved invaluable and even helped organize the final product before you now.

And as always, thank you to the Public Knowledge team for taking an idea that has been percolating for years and turning it into something tangible, and hopefully, useful.

Table of Contents

I. Executive Summary

The relationship between children and digital technology has become one of the most contentious policy debates of our time. As young people increasingly live their lives online, we see endless headlines chronicling alarming stories of cyberbullying, online predators, harmful content, and addictive design features. This tension has catalyzed a global wave of regulatory responses, from comprehensive privacy frameworks to age-appropriate design codes to outright bans on social media use by minors. Yet, many of these policy proposals struggle to sufficiently strike a balance between protecting children online and preserving free expression without cutting children off from the substantial benefits that technology platforms can offer.

When it comes to the child safety online debate, Public Knowledge's central argument is that **the most effective path forward lies not in restricting children's access to technology platforms or specific pieces of content, but in requiring technology companies to design those services with children's wellbeing as a primary consideration**. This approach – often referred to as "safety by design" – shifts responsibility from individual users and their families to the corporations that profit from the use of their online platforms. Rather than asking children to navigate exploitative systems or parents to police every online interaction, we should demand that companies build platforms that are *safe for everyone by default*.

In this report, we present a brief overview of the dominant child online safety regulatory trends in the European Union, the United Kingdom, and the United States. Based on our analysis of the pitfalls of these regulatory trends, we propose our own child online safety framework and present policy considerations to lawmakers.

II. Introduction

In June of 2025, Public Knowledge ran a workshop for high school students in partnership with the Civic Innovation Academy members of Civics Unplugged. Part of the workshop focused on how digital technology is shaping the lives of high school students and how these students wish the internet could change to serve them better. During these conversations, a clear theme emerged: a yearning for an internet that made it easier for children to make better decisions about how to use it.

They described a pattern of scrolling through endless repetitive videos that serve as meaningless distractions attributing to "brain rot," which makes it easy to lose an hour doing nothing without much notice. They knew that the algorithmic feeds are tailoring the content that they see in order to keep them on a specific app for as long as possible, however, the knowledge of this practice does not necessarily cause them to log off.

They all had stories of this pattern of behavior interfering with school, work, or other responsibilities.

At the same time, these teens value the internet. They mentioned how they were able to learn new things, access news, connect with friends, and explore burgeoning interests. What they're asking for is a fundamental shift in how platforms, apps, and websites behave – changes that encourage teens to better regulate their own behavior.

This paper draws from a thorough review of the current literature, as well as conversations with advocacy organizations, trade associations, think tanks, academics, and others who have given serious consideration to how to best protect children on the internet. While partly informed by this stakeholder consultation, our policy framework is grounded in Public Knowledge's values of free expression, the open internet, and a belief that thoughtful regulation can make the internet a positive transformative tool for communities and individuals. Based on this foundation, we propose that effective child safety legislation must prioritize youth privacy, sensible consumer protections, and evidence-based interventions.

III. Defining the Problem

Lawmakers, academics, and parents alike have decided that the kids are not alright – and the internet must be to blame. Jonathan Haidt's best-selling book, "The Anxious Generation," pins the rise in youth mental illness on cell phones and social media. Similarly, the Surgeon General's 2023[1] advisory alerts Americans about the harms of social media to young people. The very idea that technology platforms cause or exacerbate a youth mental health crisis remains a pervasive one. Recent years have seen a flood of parents suing technology platforms for allegedly facilitating egregious harms, ranging from connecting[2] kids to drug dealers peddling deadly fentanyl, to algorithmically amplifying "challenges" that persuade kids to self-asphyxiate[3] or subway surf,[4] to causing addictive[5] and compulsive use through platform design features.

---

[1] Department of Health & Human Services, Surgeon Gen. Office, *Social Media and Youth Mental Health,* Advisory Report (2023). https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf.

[2] Melissa Geber, *Parents are blaming Snapchat for their teens' fentanyl deaths. Will an LA lawsuit shape the future of social media?,* LA Times (Mar. 19, 2025). https://www.thedailynewsonline.com/lifestyles/parents-are-blaming-snapchat-for-their-teens-fentanyl-deaths-will-an-la-lawsuit-shape-the/article_2fbcc2dc-0401-11f0-a310-fbceeb8abf79.html.

[3] *Anderson v. TikTok*, No. 22-3061, 2024 WL 3948248 (3d Cir. Aug. 27, 2024).

[4] *Ashley Belanger, Meta, TikTok can't toss wrongful death suit from mom of "subway surfing" teen*, Ars Technica, (Jun. 30, 2025). https://arstechnica.com/tech-policy/2025/06/meta-tiktok-cant-toss-wrongful-death-suit-from-mom-of-subway-surfing-teen/.

[5] Matthew Bergman, Lawsuit Updates & History, Social Media Victims Law Center. (last updated Mar. 4, 2025). https://socialmediavictims.org/social-media-lawsuits/past-updates/.

To be clear, research on whether social media harms youth mental health is largely inconclusive. It would be irresponsible to attribute the youth mental health crisis to a single cause; as with most complex issues, the crisis is likely a result of a confluence of factors. While technology platforms can sometimes pose risks to children, for many users, they offer significant benefits, including access to information, opportunities for social connection, and outlets for free expression. Most children acknowledge they simultaneously have both positive and negative experiences using social media: The same kid who gets cyberbullied on Instagram may find great connections with other kids through a Discord community. Meanwhile, parents are concerned over the consequences of their kids' excessive screentime; they're noticing how social media may coincide with their children's worsening self-esteem but also feel helpless to protect them. The key takeaway is that both children *and* parents are dissatisfied with how technology platforms treat child users and are urging policymakers to take action.

The most prominent U.S. federal law focused on kids' privacy and safety online is the Children's Online Privacy Protection Act (COPPA),[6] which took effect in 2000. Over the past 25 years, the online world has changed drastically, but federal law has mostly stayed the same. Meanwhile, dominant platforms have developed increasingly sophisticated methods to circumvent the spirit of COPPA's protections while technically remaining in compliance.

As platforms developed advanced machine-learning algorithms that consume massive amounts of user data to improve ad targeting and content feed organization, they simultaneously created systematic workarounds to COPPA's requirements. The financial incentives for this circumvention are substantial: Children's data is particularly valuable because it allows platforms to build detailed behavioral profiles that predict future interests and purchasing behaviors. These profiles become increasingly valuable as children age, enabling platforms to target them with advertising throughout their development.

The most common circumvention strategy involves platforms claiming they have no "actual knowledge" of children under 13 using their services. The Federal Trade Commission discussed this in its report, "Examining the Data Practices of Social Media and Video Streaming Services."[7] This semantic sleight of hand absolves platforms from taking child privacy protective action, even when they clearly know children are using their services. Clearly, children's privacy laws need to be updated to better align with the evolution of platforms and provide adequate protections.

---

[6] 16 C.F.R § 312.

[7] Report, Federal Trade Commission, *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services* (Sept. 2024) (expanding that social media platforms routinely deny knowledge of whether a user is under 13, claiming that because their platform is not intended for children and does not allow child users, there are no children on the platform).

The challenge lies in finding the right balance of regulation – protecting kids from online harm without restricting their right to free expression. Countries, states, and localities everywhere are trying to strike this balance, but often fall short in the view of civil society and free expression groups. Some policy proposals aim to cut off children's access to technology platforms altogether while others try to target the platform's use of algorithms to organize content or apply a duty of care to uphold children's privacy standards. As illustrated in the next section, Europe and the United Kingdom have found some traction in enacting kids' safety laws, as have some U.S. states, but U.S. federal policy proposals have languished.

IV. Current State Of Regulation: Major Trends

Big Tech is experiencing a "Big Tobacco" moment[8] as regulators tighten oversight, enact stricter laws, and ramp up enforcement. Although these companies still complain of being blindsided or confused by regulations, this increased scrutiny has been developing for nearly a decade and has always included specific protections for children and teens.

The latest wave of technology-centered laws was initiated in Europe in 2016 and later in the United States, specifically in California, in 2018. While it began with broad strokes on privacy and data protection, regulators conducted extensive public consultations and issued detailed guidance on more complex compliance issues, including, in some instances, how these laws should be applied to minors. More recently, countries and states passed or are currently pursuing legislation on issues like regulation of artificial intelligence, platform liability for harmful content or design features, and children's online safety.

A. Europe and the United Kingdom

The touchstone for many child-related regulations across the globe is the 1989 Convention on the Rights of the Child, which recognizes "childhood is entitled to special care and assistance" and that the "best interests of the child are a primary consideration" in all actions and laws that affect them.[9] Among other important provisions about family integrity and preserving a child's religion and culture, the Convention declares that children have rights as *individuals* that must be protected to ensure their healthy development. For example, it prohibits "arbitrary or unlawful

[8] Lisa Macpherson, Is This Really Big Tech's 'Big Tobacco' Moment? Only Congress Can Make It So. (Oct. 29, 2021). https://publicknowledge.org/is-this-really-big-techs-big-tobacco-moment-only-congress-can-make-it-so/.

[9] Convention On The Rights Of The Child, Nov. 20. 1989, 1577 U.N.T.S. 3 (while Bill Clinton signed the treaty in 1995, the Senate never ratified it, making the United States the only UN member not a party to this convention.) https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

interference with [a child's] privacy" and directs governments to pass laws to ensure this.[10] The Convention is especially clear on the right to freedom of expression which "includes freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice."[11] It explicitly recognizes the role of "mass media" and the need to ensure that children have access to diverse information sources.[12] These principles are reiterated in tech regulations.

The European Union enacted the General Data Protection Regulation (GDPR) in 2016, which became effective in 2018. The GDPR established stricter protections for individuals and their personal information, covering key areas such as data controller obligations – like ensuring legal grounds for processing, implementing data protection by design, and maintaining cybersecurity – as well as individual rights, including the rights to consent; object to data use; and access, modify, delete, or transfer data. Two points are especially important for the current online child safety debate. First, while the GDPR recognizes several categories of data that require special consideration, it explicitly recognizes children as a vulnerable population *per se*[13] whose interests may not be adequately protected by consent, contract, or other lawful bases. Second, it directs data protection to be implemented by *design and default*, informed by necessity, risk, and context.[14]

In the intervening years, regulators have used the GDPR authorities to issue new regulations and guidelines consistent with these globally recognized human rights. For example, in 2018, the United Kingdom issued in-depth guidance on how its GDPR applies to children.[15] It made clear that the *best interests of the child* are a primary concern and that data protection impact assessments are necessary and should consider the unique risks to child data subjects.[16] The U.K. also reiterates that children have the human right to privacy and free expression, which includes access to online services and information.

---

[10] *Id.* at art. 16.
[11] *Id.* at *a*rt. 13.
[12] *Id.* at *a*rt. 17.
[13] Regulation (EU) 2016/679, art. 6(f), 2016 O.J. (L 119) https://gdpr-info.eu/art-6-gdpr/.
[14] Regulation (EU) 2016/679, art. 25, 2016 O.J. (L 119) https://gdpr-info.eu/art-25-gdpr/.
[15] Resources, The Shredding Alliance, *Guide to the General Data Protection Regulation (GDPR)* p. 245 https://www.theshreddingalliance.co.uk/wp-content/uploads/2018/09/guide-to-the-general-data-protection-regulation-gdpr-1-0-compressed-1.pdf.
[16] Guidance, Information Commissioner's Office, *When do we need to do a DPIA?* (last visited Jul. 20, 2025). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when2.

The European Data Protection Board also addressed child-friendly design in its 2020 Guidance on Data Protection by Design and Default[17] and 2024 Guidelines on the use of "significant interest" legal standard to justify data processing.[18] Now, some iteration of a general-purpose data protection law operates in 137 countries,[19] most of them with some protection for children, with many of the recent updates adopting the "best interest" framework.

Regulators' ongoing concern about children's safety online has prompted lawmakers to be more explicit about technology companies' responsibilities. In 2020, the U.K. introduced its Age-Appropriate Design Code (AADC), the first of its kind. Citing the United Nations Convention on the Rights of the Child and advancing the GDPR implementation, the AADC places on product designers the duty to prioritize children's best interests when making their products accessible to minors. Regarding data protection, the Code emphasizes providing default settings that give children the best access to online services while minimizing data collection and use. The Code elaborates extensively on the "best interest" standard, requiring platforms to design products that proactively safeguard children online by defaulting to age-appropriate experiences. Specifically, the AADC instructs developers to keep children safe from exploitation, including commercial or sexual exploitation and abuse; support children's physical, psychological, and emotional development; help children develop their views and identity; and uphold children's rights to freedom of association and play. The U.K. Design Code also highlights harms to minimize, such as physical harm, online grooming, sexual exploitation, social anxiety, bullying, exposure to harmful content, loss of control over data, excessive screen time, and economic exploitation.

Perhaps most impactful is the European Union's Digital Services Act or DSA, which went into effect February of 2024. This comprehensive regulation created by the European Commission establishes a general framework to address illegal or harmful content, which will be defined at the EU or national level through further regulation. It will operate in many ways similar to the U.K.'s children's Code, although it will provide protections for users of all ages.

Article 28 of the DSA states that, "Providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of

---

[17] Guidelines, European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Oct. 20, 2020). https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

[18] Guidelines, European Data Protection Board, *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR,* Version 1.0 (Oct. 8, 2024). https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf.

[19] Aly Apacible-Bernado & Luke Fischer, *Identifying Global Privacy Laws, Relevant DPAs*, IAPP (Mar. 19, 2024). https://iapp.org/news/a/identifying-global-privacy-laws-relevant-dpas.

privacy, safety, and security of minors, on their service." It goes on to prohibit profiling-based advertising to minors; clarifies that platforms are *not* required to process additional information when determining the age of a user; and permits the European Commission to issue guidelines defining the appropriate and proportionate measures required.

In 2024, the European Commission started the rulemaking process as required by the DSA after issuing a call for evidence to support more specific guidelines for the protection of children.[20] The Commission signaled its intention to regulate broadly by incorporating the Organization for Economic Cooperation and Development's (OECD) 2021 typology of risks for children in the digital environment: harmful content, conduct, contact, consumer practices, and cross-cutting risks.[21] The call for evidence also endorsed the use of a special Children's Rights Impact Assessment, a process UNICEF has developed over the last several years.[22]

This is not an exhaustive list of international efforts to regulate how companies interact with children and their data. We provide these examples to demonstrate where the rest of the world is headed – regardless of what the U.S. does next – and to note important trends. Regulators are thinking expansively about both the harms and benefits that may follow the use of digital products. For years, companies have been on notice that they are responsible for more than just mitigating user privacy risks and should think holistically about how children experience their products.

B. Domestic Trends In Child Safety Regulation

U.S. regulators have pursued new laws and regulations in fits and starts over the last decade. States have been particularly active in passing privacy laws, and in recent years, a handful have adopted age-appropriate design codes and bans on social media use by minors without parental consent. The federal government, on the other hand, has floundered, unable to pass any substantive reform, privacy-related or otherwise; even though federal agencies and Congress have both expressed interest in doing so. Ultimately, domestic gains have been quite modest. The good news: The U.S. is slowly moving away from notice and consent as a framework and towards corporate

---

[20] European Commission, Protection of Minors Guideline (adopted Jul. 14, 2025). https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14352-Protection-of-minors-guidelines_en.

[21] Organisation for Economic Co-operation and Development, DSTI/CDEP/DGP(2020)3, Children in the Digital Environment: Revised Typology of Risks, Unclassified (Jan. 12, 2021). https://one.oecd.org/document/DSTI/CDEP/DGP(2020)3/FINAL/en/pdf.

[22] UNICEF, Developing Global Guidelines for Child Rights Impact Assessments in Relation to the Digital Environment, Summary (Apr. 2024). https://www.unicef.org/media/156046/file/Child%20Rights%20Impact%20Assessments%20in%20Relation%20to%20the%20Digital%20Environment.pdf.

responsibility. The bad news: Some lawmakers are committed to categorically limiting children's access to social media or other online services, to the detriment of a child's freedom of expression.

1. *Privacy: Federal*

Congress came out swinging against Facebook, now known as "Meta," in the wake of the 2018 Cambridge Analytica scandal, where a political consulting firm collected data from up to 87 million Facebook users without informed consent. Committees held dozens of hearings in the subsequent years to inquire about corporate data collection, use, and sharing practices in the consumer sphere with a focus on the largest tech companies. Representatives and senators from both parties authored comprehensive privacy legislation. Most of these federal bills attempted to cover the same topics as the GDPR, but in U.S. legal terminology and often with a lighter regulatory touch, including more transparency, better consent mechanisms, data security baselines, minimization requirements, and user rights. Ultimately, these bills failed in the political arena, primarily due to corporate resistance to accountability measures, especially the right for consumers to pursue judicial review.

Congress eventually shifted its focus from broad privacy issues to specifically child privacy concerns, with many believing that any forthcoming privacy legislation would likely be an update to the Children's Online Privacy Protection Act (COPPA). It's important to understand what COPPA is and what it is not. While it's often said to require parental permission for children to use online services, it actually has a more limited scope: It mandates that companies obtain parental permission to collect, use, and share personal information from children under 13. The law also includes other provisions like data minimization, which went unexamined and unenforced for decades as regulators focused mainly on the quality of the parental consent process.

Bills aiming to reform COPPA often share common themes. First, many lawmakers believe that 13 is not the suitable age to assign minors adult legal responsibilities and consequences. As a result, proposed legislation increases the age threshold to 16, with teens typically exercising opt-in and other rights from ages 13 to 15. Many bills also revise the knowledge requirement that activates COPPA obligations. Instead of restricting COPPA to services directed at children under 13 or when a service has actual knowledge that a user is a child, these bills suggest a constructive knowledge standard. This means companies must provide protections if they should have known the user was a minor.[23] Despite several markups, none of these bills have become law.

The Federal Trade Commission initiated the process of issuing explicit data privacy and security regulations under its authority to investigate and punish unfair and deceptive

[23] Chloe Altieri, *Now, On the Internet, Will Everyone Know if You're a Child*? FUTURE OF PRIVACY FORUM (May 13, 2024). https://fpf.org/blog/now-on-the-internet-will-everyone-know-if-youre-a-child/.

commercial practices, as outlined in the FTC Act. Despite engaging in an exhaustive notice and consultation process under the Biden administration, the FTC was ultimately unable to enact new data protection regulations[24] and passed only a modest set of clarifications to COPPA in January of 2025.[25] For example, the new COPPA rule clarifies that the longstanding requirement to delete children's data after it is no longer necessary means that, "Personal information collected online from a child may not be retained indefinitely." As noted by FTC Commissioners Alvaro Bedoya and Rebecca Kelly Slaughter, the Biden administration had to bring enforcement actions to compel mega-corporations like Microsoft and Amazon to stop retaining children's data *forever*.[26] This important clarification can also be seen as a wake-up call regarding the likelihood of federal regulation.

2. *Privacy: State*

California legislators passed the first-in-the-nation U.S. data protection law under the California Privacy Act (which created the California Privacy Protection Agency) in 2018[27] and California voters strengthened it in 2020 through a referendum. Unprecedented in depth and breadth, the California Privacy Rights Act incorporated many concepts from the GDPR, filtered through the language of the American legal system. Nineteen U.S. states now have baseline privacy laws, although most have not adopted California's framework for their legislation.[28]

States are taking several approaches to protecting children's data. The first is simply raising the age at which a user is considered an adult for data processing and therefore no longer subject to enhanced protections. California is one such example as it raised the threshold from 13 to 16 years of age. Other states maintain the 13-year-old threshold but add additional protections for these younger users. Virginia, for example, prohibits targeted advertising, profiling with legal effects, and selling personal data for this age group.[29] And finally, still other states focus on creating new protections for teens. The New York Child Data Protection Act requires companies to follow COPPA for

---

[24] Commercial Surveillance and Data Security Rulemaking, 87 Fed. Reg. 51273 (proposed Aug. 8, 2022). https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking.

[25] Press Release, Fed. Trade Comm'n, *FTC Finalizes Changes to Children's Privacy Rule Limiting Companies' Ability to Monetize Kids'* Data (Jan. 16, 2025). https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data.

[26] Statement of Comm'r Alvaro M. Bedoya, joined by Comm'r Rebecca Kelly Slaughter, Federal Trade Commission, *Notice of Final Rulemaking to Update the Children's Online Privacy Protection Rule (COPPA Rule*) (Jan. 16, 2025). https://www.ftc.gov/system/files/ftc_gov/pdf/bedoya-coppa-statement-2025-01-16.pdf.

[27] Cal. Civ. Code § 1798.199.10 (establishing the California Privacy Protection Agency).

[28] IAPP, *U.S. State Privacy Legislation Tracker 2025* (last updated Jul. 7, 2025). https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf.

[29] VA. Code Ann. § 59.1-575 (effective Jan. 1, 2026)

children under 13, requiring parental consent before collecting data; but for children 13 to 17, obtain consent from the child directly for any data processing that is not strictly necessary to serve the product requested by the teen.[30]

3. Child Online Safety: Federal

American regulators have also pursued more substantive limitations on corporate behavior although proposals are significantly narrower than those in the U.K. or EU. Like privacy, these efforts have stalled at the federal level but the Kids Online Safety Act (KOSA) received bipartisan support in the U.S. House and Senate last year and passed through committees of jurisdiction in both houses.[31] On the Senate floor, it passed nearly unanimously by a vote of 91-3. As it was reintroduced summer of 2025, the bill would require online platforms to take reasonable care to avoid design features that encourage reasonably foreseeable harms to minors under 16, such as eating or substance use disorders, suicidal behavior, compulsive tech usage, and more.[32] Given the broad support it received in the last Congress, it is likely the bill will be considered again.

The U.S. Senate Commerce Committee also passed the Kids Off Social Media Act (KOSMA) in February.[33] The bill prohibits social media companies from allowing known children under 13 to create accounts and directs them to delete any such accounts already in existence. It further bans the use of personalized recommendation systems based on the data of children or teenagers. Nonprofit advocacy organizations widely oppose this bill due to its First Amendment and privacy incursions,[34] and it has yet to be scheduled for Senate floor consideration.

4. Child Online Safety: State

Like in privacy, the states are moving forward with new child safety online regulations quickly, focusing on two areas: age-appropriate design codes and limiting access to certain online products like social media.

---

[30] S. 7695A, 2023-2024 Leg., Reg. Sess. (N.Y. 2023) https://www.dwt.com/-/media/files/blogs/privacy-and-security-blog/2024/06/s7695b.pdf?rev=ca6696b9c23a4f75949898a08e337f77&hash=CA6A91DE8A1AC12C66590F21D455E803.

[31] S. 1748, Kids Online Safety Act, 119th Cong. (2025) https://www.congress.gov/bill/119th-congress/senate-bill/1748/text.

[32] S. 1748, Kids Online Safety Act, 119th Cong. (2025) https://www.congress.gov/bill/119th-congress/senate-bill/1748/text.

[33] Kids off Social Media Act, s. 278, 119 Cong. (2025) https://www.congress.gov/bill/119th-congress/senate-bill/278/text.

[34] Letter from Open Tech. Inst. & ACLU to S. Comm. on Com., Sci., & Transp. (Feb. 3, 2025). https://newamericadotorg.s3.amazonaws.com/documents/Letter-on-KOSMA_250203.pdf

California passed the first U.S. AADC in 2022, followed by Maryland in 2024,[35] and Nebraska and Vermont in the summer of 2025.[36] They differ in language, but all generally contain some requirements for data minimization and high default settings. California's is the most comprehensive, borrowing heavily from the U.K. law, with Maryland close behind. Vermont and Nebraska are substantially narrower: Nebraska does not address "best interests" or duties of care at all, instead focusing on user controls for the child. Vermont, on the other hand, relies on a very short list of harms – emotional distress, compulsive use, and discrimination – with caveats to protect First Amendment activity.

In March of 2025, the Northern District of California granted a preliminary injunction to tech trade association NetChoice against California's AADC. That court found that the challenge was likely to succeed on First Amendment and vagueness grounds.[37] Surprisingly, one of the most contentious issues in the case was the requirement to complete a data protection impact assessment. Data protection assessments have long been part of different privacy laws, like the GDPR. They have been conceived of as a way to both create incentives for companies to mitigate risks early in the data collection process, and also provide transparency for regulators.[38] In the case of California's AADC, the assessment in question not only required companies to review their data collection and design decisions, but to also determine whether they were exposing children to harmful content. The Ninth U.S. Circuit Court of Appeals found that this assessment of content would not survive First Amendment scrutiny because it "deputized covered businesses into serving as censors for the State."[39]

Other states, instead of using a design-code style law, are instead attempting to limit minors' access to social media entirely. These bills take one of two forms: They either ban children from using social media altogether *or* ban its use without explicit parental consent. States do not agree about what age children or teens can join social media sites without permission, with current and pending laws lifting social media restrictions for those between the ages of 13-18.

---

[35] Future of Privacy Forum, Comparison of California Age-Appropriate Design Code Act & Maryland Age-Appropriate Design Code Act (Apr. 2024). https://fpf.org/wp-content/uploads/2024/04/AADC-Comparison-Chart-California-vs.-Maryland-4.28.24.pdf.
[36] Future of Privacy Forum, Comparison of Nebraska Age-Appropriate Design Code & Vermont Age-Appropriate Design Code (Jun. 2025). https://fpf.org/wp-content/uploads/2025/06/FPF-AADC-Comparison-Chart-Nebraska-vs.-Vermont.pdf.
[37] Net Choice, LLC v. Bonita, NO. 22-cv-08861-BLF (N.D. Cal. Mar. 2025) https://netchoice.org/wp-content/uploads/2025/03/NetChoice-v-Bonta-CA-Speech-Code-PI-Granted-Mar-13-2025.pdf.
[38] Info. Comm'r's Off., How Do We Do DPIA? https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/.
[39] Net Choice, LLC v. Bonita, 113 F.4th 1101, 1118 (9th Cir. 2024)

It is important to note that many of these proposals, whether design codes, social media bans, or other targeted regulation of online content, require platforms to engage in age assurance or verification: some defined level of effort to determine the age of a user in support of age-gating decisions. Many require "reasonable efforts" and clarify that companies should not engage in privacy-invading tactics to determine a user's age. Several are subject to litigation now. Most notably, a Texas law requiring age verification for access to online pornography was upheld by the U.S. Supreme Court in June of 2025.[40]

V. Public Knowledge Principles on Child Safety Regulation

Child online safety regulations have momentum, and lawmakers are unlikely to let these issues go anytime soon. Given the potentially exploitative behavior of companies that hold our data, the concern is justified; however, regulating in this space is challenging. While our preference would be to see a comprehensive privacy law protecting all internet users enacted at the federal level first, before specific regulations directed at children's use of the internet, the political reality necessitates us weighing in on this debate.

Public Knowledge urges lawmakers to keep in mind the ultimate goal: to build an internet that is safe for everyone, empowers users, and holds corporations accountable for harming people. To this end, we propose the following principles for U.S. policymakers to consider when writing child privacy and safety legislation:

- The internet has the potential to enrich children's lives. It is easy to get lost in the shocking revelations of bad corporate behavior, but it is imperative to remember that the internet can facilitate learning, play, relationships, civic engagement, self-exploration, and other necessities of childhood. Given that digital technology, including artificial intelligence, is being woven into every aspect of our lives, we need regulations that provide an on-ramp that encourages digital literacy and technological fluency as children grow into adulthood.

- Safe product design is essential for products children will use. No amount of transparency or consent can mitigate the harms that come from products that are designed to exploit users and their data by default. Systemic change will only occur when corporations are compelled to design products with features that protect children as well as adults – and those features are activated by default.

- Empowered young people are best positioned to make decisions about their internet use. Parents have a primary role in raising savvy and responsible

[40] *Free Speech Coal., Inc. v. Paxton, 145 S. Ct. 2291 (2025)* https://www.supremecourt.gov/opinions/24pdf/23-1122_3e04.pdf

internet users. However, lawmakers should resist the temptation to view parental consent as a solution to poor product design. Safe design and protective defaults will provide guardrails and protect children from corporate exploitation.

- Regulations should be risk-based and focus on the practices or features that are most likely to cause harm. Regulations that are an inch deep and a mile wide won't serve children by throwing away all positive elements of their use of online platforms due to some negative elements. Instead, product developers should be clearly directed to address the most likely and most serious harms.

- Meaningful enforcement regimes include the ability to petition a court for redress. Many important rights have been won in the courthouse, not the statehouse. It is crucial that children and their representatives be able to assert their rights before neutral judges and not rely solely on the priorities and resources of government agencies and politicians.

- Regulations should avoid banning categories of content or access to online products. Children have human and constitutional rights to privacy and freedom of expression; outright bans are likely to infringe upon these rights. Bans are also inconsistent with a risk-based approach that recognizes that not all online experiences pose the same level of risk, and that protections should be proportionate to the likelihood of harm.

- Continued research is necessary to ensure that regulation is tailored and effective. Good regulation is informed by fact, and while we are learning more every day about how online products work and their effect on children, there remain significant gaps in our understanding. Continued research helps identify which specific features or practices pose real risks, which are beneficial, and how these impacts vary across age groups, contexts, and individual experiences. Therefore, transparency requirements as well as privacy-protective researcher access rights should be considered part of the suite of tools legislators have to address child safety.

These principles do not call for a focus on specific content that may or may not be harmful to children, but rather a structural approach to regulation that provides the necessary incentive changes to create a better experience for all internet users. Focusing on consumer protection tools like privacy laws and design decisions provides a cleaner legal footing, and will also be more effective at creating long-term change.

VI. Policy Considerations for Lawmakers

We recommend policymakers consider the following factors when developing policies intended to make the internet better for child users:

A. Structural questions

1. Who is a child?

There is overwhelming agreement that the original COPPA threshold kicking 13-year-olds into legal and digital adulthood – especially in the U.S. consent-based model – no longer makes sense. Child and teen development is a continuum, not a cliff, and smart regulation will recognize that. We encourage lawmakers to use a risk-based model to minimize barriers and incorporate the following factors:

- Smart design instead of a magic number: The more regulation puts the onus back on corporations to design safe products with high defaults, the less important it is to find the right age to access the internet unrestricted.

- Risk-based analysis of products or features: To the extent there will continue to be additional protections for young people, the highest standards should focus on the riskiest products and features. For example, apps or websites that allow minors to post publicly or share their personal information broadly are justified in having a higher age gate. Low-risk products like child directed games or videos without a social networking component can be lower. Tailoring age requirements will benefit everyone in the ecosystem: Young people will have access to products, corporations will have the freedom to innovate, and regulators and parents can focus on setting and enforcing standards that are meaningful.

- Glide path to online adulthood: Lawmakers should take inspiration from the U.K.'s age-appropriate design code to think of protections and controls that align with the known developmental stages of children and teens. In short, instead of a single on-off switch, regulation could have the strictest protections for young children and more moderate options for users up to 18 years old. As we discuss more below, parental controls should wane as a minor ages.

2. *Should age assurance technology be used to restrict minors' access to lawful content?*

While Public Knowledge disagrees with the Court's decision in *Free Speech Coalition v. Paxton*,[41] privacy-preserving age assurance technology can be used for non-content-based policy requirements. This can include requiring more privacy protections for minors or restricting specific features in general audience websites or applications from use by youth because those apps pose heightened risks to children. Focusing on distinct features or design decisions, rather than specific pieces of content, has two major benefits. First, any child-specific privacy or safety law without content restrictions is much less likely to be overturned on First Amendment grounds. The Supreme Court made clear in the NetChoice cases[42] that not all forms of tech regulation touch expression. Therefore, laws that do not restrict the accessibility of lawful speech should not be subject to the same scrutiny under the First Amendment as laws that do.[43] Second, requirements to remove content, even if found lawful, can cause precautionary over-enforcement. Overbroad bans frequently filter out educational, scientific, or health-related content due to false positives or misclassification.[44] This not only limits minors' ability to explore legitimate topics, but may also erode trust in the moderation system for adults. As states continue to iterate on different child safety models, we urge legislators to abandon a model that requires differing treatment of lawful content. There are more productive avenues for legislation that provide more direct protections to children without abandoning the benefits of the internet.

3. *What age assurance processes are sufficient?*

Corporations, policy advocates, and policymakers want more clarity about *how* a platform should determine who is a child. Some are concerned that children may lie to access inappropriate content; others note platforms have willfully ignored signs that children are using their products. If a law is to signify the quality of age assurance processes, then it should consider:

- Smart design instead of notice and consent: We'll say it again: Shift the responsibility to corporations to design safe products with the highest defaults for the largest group of people. Age divisions only matter if a corporation insists on offering risky or exploitative features to adult users. It is, of course,

[41] Public Knowledge, *Protecting Kids Shouldn't Mean Weakening the First Amendment* (Jul. 2025). https://publicknowledge.org/protecting-kids-shouldnt-mean-weakening-the-first-amendment/
[42] *Moody v. Netchoice, LLC*, 603 U.S. 707 (2024)
[43] Public Knowledge, *Platform Regulation after the Supreme Court's NetChoice Ruling* https://publicknowledge.org/platform-regulation-after-the-supreme-courts-netchoice-ruling/ (Jul. 2025)
[44] Tara Garcia Mathewson, *Schools Were Just Supposed to Block Porn. Instead They Sabotaged Homework and Censored Suicide Prevention Sites*, THE MARKUP (Apr. 13, 2024). https://themarkup.org/digital-book-banning/2024/04/13/schools-were-just-supposed-to-block-porn-instead-they-sabotaged-homework-and-censored-suicide-prevention-sites

appropriate to have adult-oriented products, but smart design across the board can relieve much of the burden of getting age assurance just right.

- Risk-based standards instead of blanket requirements: Some products are simply lower risk and errors in age gating may not result in any harm. For these products or features, age assurance can be lower.

- Privacy and security for additional age assurance processing: Many laws are clear that platforms are not required to collect or process additional information to determine age if it is unnecessary to do so. To the extent that a platform or a third party processes new information to determine a user's age, that information can be protected by minimization and smart security practices. For example, platforms should be required to delete any additional information processed to determine age and be prohibited from sharing age information with third parties.

4. *What knowledge must a platform have that a user is a child to trigger heightened obligations?*

Determining exactly what knowledge requirements to include in new child online safety proposals triggers additional controversy. This is a component of all law and regulation, regardless of the topic, but has become a sticking point that, in some instances, has prevented both child safety and privacy legislation from passing at all. The challenge lies in how "knowledge" is defined and applied, particularly when companies already use age-related information for commercial purposes like delivering personalized ads or recommending products. It would be unreasonable for a company to have sufficient confidence that a user is a child to target them with personalized ads and content, yet claim insufficient certainty about that same user's age when facing regulatory accountability for child protection. Lawmakers could discourage this bad faith behavior by clarifying that knowledge is demonstrated by choosing to categorize a user as a child for purposes of advertising or product recommendations.

B. By the Issue

1. *Bans on access*

The most worrying trend in the U.S. concerns completely banning child or teen access to social media or other general audience online products. This is never the appropriate policy response. It punishes *consumers* instead of the *companies* that design risky products – especially targeting children and teens but also those users who are of age but unable or unwilling to satisfactorily prove it. It is also inconsistent with the modern

understanding of child and teen development and the principle of a risk-based approach that minimizes compliance and enforcement burdens.

Besides, as we discussed above, these proposals have been challenged in court and some judges are issuing injunctions as arguments on the full merits proceed. Regulators who want to make a difference now should legislate in a more tailored fashion or risk having the entirety of their child safety legislation determined unconstitutional by the courts.

2. *Balancing parental and children's rights*

Many proposals, especially the bans discussed above, do not actually alter corporate behavior or result in safer online products. They just change who checks the box on the consent pop-up, with business continuing as usual. This does not benefit children, teens, or their parents. It may be tempting to take this shortcut in the name of asserting parents' rights, but everyone would be better served by focusing on safer product design, high defaults, transparency, and more targeted parental controls. Importantly, this respects the privacy and expression rights of children and teens but also directs parents' attention to the most important decisions that actually impact child safety online.

3. *Privacy*

In both comprehensive privacy proposals, as well as child specific proposals, the protections cannot rely on notice and choice as the operative framework. As we noted in our comment to the FTC,[45] it gives users the illusion of control while they are presented with a "take it or leave it" proposal. It also lets corporations shirk responsibility for product design decisions and avoid building a safer internet for children and all users. To this end, regulators should focus on changing corporate data collection and use practices. Whether the underlying legislation is a comprehensive data protection bill or a bill narrowly focused on children's privacy, regulators should prioritize data minimization and purpose limitations by design.

4. *Safety by design and default*

We urge decision makers to remember that the single most important thing they can do in child-related legislation is to put the onus on corporations – not kids, and not their parents – to design a better online experience. Holding corporations to account has been part of the law for decades, although it has not always been a priority for enforcement. Recent trends to more explicitly revisit this requirement in the child privacy

[45] Sara Collins et. al., Public Knowledge & Yale L. Sch. Tech Accountability & Competition Project, Comments from Public Knowledge and the Yale Law School Tech Accountability & Competition Project, Docket No. FTC-2022-0053-0001 (Nov. 2022). https://publicknowledge.org/wp-content/uploads/2022/11/Commercial-Surveillance-Comments-2.pdf

and safety policy space are promising. Lawmakers should feel particularly confident in including data minimization requirements and mandates to set children's accounts to the most protective defaults, which serve as the baseline for most, if not all, recent legislation. They should also consider explicitly putting their thumb on the scale when it comes to monetizing children's data and attention by, for example, limiting push notifications and prohibiting targeted advertising to this age group. Other components of a child safety and privacy bill could include directives for easy-to-understand, child-centered controls, defaults to avoid public posting or public sharing of personal information, and for limiting private communication with unfamiliar adults.

5. Regulating Algorithms

As understanding grows about how online platforms employ engagement-maximizing algorithms to target and organize content, and how these algorithms might exacerbate harm by promoting harmful material, it is understandable that proposals are being made to control how these algorithms are trained and deployed. However, we caution against going after how algorithms curate content rather than tackling the underlying harms. For one, proposals may risk running afoul of First Amendment protections, especially as courts view algorithmic curation as a form of protected editorial speech.[46] More fundamentally, focusing specifically on algorithms creates an arbitrarily narrow regulatory approach that can be easily circumvented – if a user or community is harmed through a platform's choice to amplify disinformation, it shouldn't matter whether this was accomplished by an algorithm, other software, or human decision-making.[47] The harm remains the same regardless of the method used to create it. Finally, while transparency about algorithmic processes can be valuable, it should serve as a foundation for better-informed regulation rather than a substitute for addressing the business practices and design choices that create harmful outcomes in the first place.

VII. Policy Proposals

A. Age Assurance for High-Risk Features

Rather than implementing blanket age verification requirements for accessing *any* online platform, we recommend that policymakers propose a risk-based standard that scales with the potential harm associated with specific features.

---

[46] Electronic Privacy Info. Ctr., *In Net Choice Cases, Supreme Court labels a Suprisingly Narrow Class of Online Platform Company Activties as Protected* Expression (Jul. 10, 2024). epic.org/in-netchoice-cases-supreme-court-labels-a-surprisingly-narrow-class-of-online-platform-company-activities-as-protected-expression/

[47] Public Knowledge, *Should Algorithms Be Regulated? Part 3: Evaluating Alternative Frameworks for Regulating* Algorithms (Nov. 16, 2022). https://publicknowledge.org/should-algorithms-be-regulated-part-3-evaluating-alternative-frameworks-for-regulating-algorithms/

Recommendation: Propose a tiered risk assessment framework that would require platforms to classify features by potential harm to minors, which could look like:

- Low Risk: Access to basic content browsing, educational resources, and general communication features is *not* age gated.
- Medium Risk: Age assurance using available data sources (i.e. "age estimation") may be appropriate to access social networking, interact with user-generated content, and receive algorithmic recommendations.
- High Risk: Strict age assurance could be required to access adult content, including pornography. Other features particularly risky for children include those that enable unwanted connections with strangers or live video streamed outside a user's friend network.

Age verification technologies for high-risk features must be privacy-preserving. Platforms should be required to implement verification methods that prove age without exposing personal information (known as "zero-knowledge" proofs). In other words, platforms should be prohibited from sharing age information with third parties and should be required to delete any additional data collected for age-determination purposes.

An important enforcement mechanism would clarify that platforms demonstrate knowledge of a user's age when they categorize that user as a child for advertising or product recommendation purposes, thereby preventing companies from claiming ignorance while simultaneously targeting children for commercial purposes.

B. Default Privacy Settings

Recommendation: Mandate that accounts for users under 18 years default to the highest privacy and safety settings available.

Platforms should make it so:

- Users must initiate changes to make their accounts public.
- Users must explicitly choose to share personal information with third parties.
- Geolocation features are disabled by default.
- Automatic discovery by phone number, email, or other identifiers is disallowed.
- Profile information visibility to non-friends is limited.

Default settings would serve as a baseline protection for the largest group of users, with the burden placed on platforms to justify any features that might require different settings. Furthermore, privacy policy proposals should emphasize data minimization

and purpose limitations built into the system architecture, rather than rely on user choices.

C. Mandatory Breaks from Continuous Content Applications

As mentioned in the introduction of this paper, there have been significant concerns by both teens and researchers[48] that passively consuming continuous personalized content can contribute to increased rates of digital fatigue and lost time.

Recommendation: Policymakers should mandate that platforms implement regular, non-bypassable wellness breaks for users younger than 18 for websites and applications that provide continuous, personalized content. The length of the wellness break may be determined in consultation with relevant researchers and health professionals.

The design of many applications encourages endless scrolling with minimal natural stopping points, creating an environment where users (especially younger ones) can easily lose track of time. This behavioral pattern has been linked to disrupted sleep schedules and reduced focus. To address this, platforms should be required to implement an automated five-minute pause after each hour of continuous use. This pause would serve as a digital cue to reset, reflect, and nudge users toward healthier usage habits.

D. Reducing Interactions with Unknown Accounts or Unwanted Contacts

To protect youth users from unsolicited and potentially harmful interactions, applications and websites that allow users to have friends, groups, or other types of followings should be required to implement friction points that slow or prevent contact from unknown accounts. This can make platform interactions safer without unduly disrupting the communication abilities of users.

Recommendations:

- Require users to approve message requests before viewing any content, especially visual media.
- Add warnings for accounts with no mutual connections or suspicious traits.
- Provide easy access to blocking tools, including bulk blocking (e.g. blocking all accounts tied to a harmful post or pattern).

---

[48] Vaishnavi S. Nakshine et al., *Increased Screen Time as a Cause of Declining Physical Psychological Health, and Sleep Patterns: A Literary Review, Cureus* (Oct. 2022). https://pmc.ncbi.nlm.nih.gov/articles/PMC9638701/

- Allow users to mute individuals, threads, or keywords to manage their own exposure to content they would rather not interact with.
- Ensure reporting tools are fast, simple, and transparent, with clear follow-up for users.
- Hide child user accounts from public visibility and discoverability.

While many platforms have implemented some of these features, being legally required to implement them will ensure that all platforms have all of these features. These interventions prioritize youth consent, autonomy, and safety, while not materially inhibiting the ability to connect with others.

E. Researcher Access

It is futile to categorize platform design features by harm if we do not understand how the features themselves function, and how users interact with those features.

Recommendation: Facilitate researcher access to platform data to ensure policy proposals are based on evidence.

This could look like:

- University-based “cleanrooms” for sensitive data analysis.
- Requiring platforms to provide privacy-preserving synthetic datasets for broad research where individual-level data isn’t necessary, like assessing *general* social media usage patterns among teens during certain time periods, or measuring effectiveness of content moderation policies.
- Sharing data on the effectiveness of safety measures, including parental controls, content filters, and design modifications.

VIII. Conclusion

This report reviews the legal regimes (both here and abroad) to identify a path forward that offers real accountability without sacrificing the benefits of the internet for children. That includes safety by design, privacy-by-default settings, and clear obligations for websites, applications, and platforms. As demonstrated by this report, policymakers must resist overly-broad content bans or blunt age restrictions, and instead focus on features and practices most likely to cause harm. Simply banning all children from the internet is both unrealistic and undermines their First Amendment rights to free expression – instead, lawmakers should seize this political opportunity to pass legislation centered on the healthy development, safety, and expression of *every* child.