



March 18, 2025

Arkansas Senate
Attn: Judiciary Committee
500 Woodlane Street, Suite 320
Little Rock, Arkansas 72201-1090

Re: HB 1717 - "Children and Teens' Privacy Protection Act" (Oppose)

Dear Chair Clark and Members of the Senate Judiciary Committee:

[On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 1717. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.¹ Proposed regulations on the interstate provision of digital services therefore can have a significant impact on CCIA members.

CCIA firmly believes that children are entitled to greater security and privacy online. Our members have designed and developed settings and parental tools to individually tailor younger users' online use to their developmental needs. For example, various services allow parents to set time limits, provide enhanced privacy protections by default for known child users, and other tools allow parents to block specific sites entirely.² This is also why CCIA supports implementing digital citizenship curricula in schools, to not only educate children on proper social media use but also help teach parents how they can use existing mechanisms and tools to protect their children as they see fit.³ However, the proposed bill would require businesses to collect more sensitive data about users of all ages, jeopardizing their privacy and creating compliance burdens that will be difficult for businesses to meet and worsen consumer experiences. The bill presents the following concerns:

Age verification and parental consent requirements raise significant privacy concerns.

Every approach to age determination presents trade-offs between accuracy and privacy⁴—in addition to significant costs, especially for startups⁵—and there is no one-size-fits-all approach. Different services consider various factors, including but not limited to their user base, the service offered, risk calculation, privacy expectations, and economic feasibility. A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*,

¹ For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than \$100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at <https://www.ccianet.org/members>.

² Competitive Enterprise Institute, *Children Online Safety Tools*, <https://cei.org/children-online-safety-tools/>.

³ Jordan Rodell, *Why Implementing Education is a Logical Starting Point for Children's Safety Online*, Disruptive Competition Project (Feb. 7, 2023), <https://project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/>.

⁴ Kate Ruane, *CDT Files Brief in NetChoice v. Bonta Highlighting Age Verification Technology Risks* (Feb. 10, 2025), <https://cdt.org/insights/cdt-files-brief-in-netchoice-v-bonta-highlighting-age-verification-technology-risks/>.

⁵ Engine, *More than just a number: How determining user age impacts startups* (Feb. 2024), <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/65d51f0b0d4f007b71fe2ba6/1708465932202/Engine+Report+-+More+Than+Just+A+Number.pdf>.

contains guiding principles for age assurance and discusses how digital services have used such principles to develop best practices.⁶

The proposed bill does not meet these standards. In particular, the proposed overcollection of data about children would make kids less safe, requiring the collection and storage of sensitive data that could be exploited. For example, the real-time data access requirement would undermine privacy and make children less safe, as developers would have access to sensitive personal information identifying an app store provider's users, including parents of their underage customers. Such excessive monitoring has been shown to negatively affect young people's mental health and development.⁷

The proposed bill suggests imposing a government-mandated requirement to verify all Arkansas users' ages that conflicts with data minimization principles ingrained in standard federal and international privacy and data protection compliance practices.⁸ Determining a user's age and verifying parental consent inherently requires collecting additional sensitive data from those users, and any document capable of verifying a user's age will likely contain sensitive information. Requiring companies to collect more user data even as other states require collecting less data places businesses in the untenable position of picking which state laws to comply with, and which to unintentionally violate.⁹

The Commission Nationale de l'Informatique et des Libertés (CNIL) analyzed several existing online age verification solutions but found that none of these options could satisfactorily meet three key standards: 1) providing sufficiently reliable verification; 2) allowing for complete coverage of the population; and 3) respecting the protection of individuals' data, privacy, and security.¹⁰ Though the intention to keep kids safe online is commendable, this bill undermines

Age determination and parental consent requirements for online businesses are currently being litigated in several jurisdictions.

When the federal Communications Decency Act was passed, there was an effort to sort the online population into children and adults for different regulatory treatment. That requirement

⁶ *Age Assurance: Guiding Principles and Best Practices*, Digital Trust & Safety Partnership (Sept. 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.

⁷ See, e.g., Hannah Quay-de la Valle, *The Chilling Effect of Student Monitoring: Disproportionate Impacts and Mental Health Risks*, Ctr. for Democracy & Tech. (May 5, 2022), <https://cdt.org/insights/the-chilling-effect-of-student-monitoring-disproportionate-impacts-and-mental-health-risks/> (finding that "Monitoring programs, if not carefully implemented, can stifle growth and leave students vulnerable to the chilling effect, placing their mental health at risk").

⁸ See, e.g., *Fair Information Practice Principles (FIPPs)*, Fed. Privacy Council, <https://www.fpc.gov/resources/fipps/>; see also *Principle (c): Data Minimisation*, U.K. Info. Comm'r Off., <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/>.

⁹ Caitlin Dewey, *California's New Child Privacy Law Could Become National Standard*, The Pew Charitable Trusts (Nov. 7, 2022), <https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/11/07/californias-new-child-privacy-law-could-become-national-standard>.

¹⁰ *Online Age Verification: Balancing Privacy and the Protection of Minors*, CNIL (Sept. 22, 2022), <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>.



was struck down by the U.S. Supreme Court as unconstitutional because of the infeasibility.¹¹ After 25 years, age authentication still remains a vexing technical and social challenge.¹²

Recent state legislation that would implement online age verification or estimation and parental consent measures is currently facing numerous constitutional challenges, and numerous federal judges have placed laws on hold until these challenges can be fully reviewed, including in Arkansas, California, Mississippi, Ohio, Tennessee, Texas, and Utah.¹³ CCIA anticipates that these forthcoming rulings may clarify which age determination requirements are Constitutionally permissible. CCIA therefore recommends that lawmakers permit this issue to be more fully examined by the judiciary before burdening businesses with legislation that risks being invalidated and passing on expensive litigation costs to taxpayers.

HB 1717’s data collection prohibitions encompass much non-sensitive data, limiting businesses’ ability to improve their products and services without improving user privacy.

All of HB 1717’s restrictions on data collection treat sensitive and non-sensitive personal information alike. For instance, HB 1717 places the same restrictions on businesses who process an individual’s first and last name as those who process a social security number. While the protection of children and teens’ sensitive information is a worthy goal, imposing excessive restrictions on non-sensitive personal information merely inhibits businesses’ ability to improve their products and services without any corresponding benefit to user privacy. CCIA therefore recommends that restrictions on the processing of personal data be limited to categories of sensitive information that pose a risk to users if disclosed.

* * * * *

While we share the concerns of the sponsor and the Senate Judiciary Committee, we encourage Committee members to resist advancing legislation that is not adequately tailored to this objective. We appreciate the Committee’s consideration of these comments and stand ready to provide additional information as the Legislature considers proposals related to technology policy.

Sincerely,

Tom Mann
State Policy Manager, South
Computer & Communications Industry Association

¹¹ *Reno v. ACLU*, 521 U.S. 844, 855-57, 862 (1997).

¹² Jackie Snow, *Why age verification is so difficult for websites*, Wall St. J. (Feb. 27, 2022), <https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728>.

¹³ See, e.g., *NetChoice v. Bonta*, No. 24-cv-07885, 2025 WL 28610 (N.D. Cal. Jan. 2, 2025); *NetChoice v. Bonta*, No. 22-cv-08861, 2024 WL 5264045 (N.D. Cal. Dec. 31, 2024); *NetChoice, LLC v. Reyes*, No. 23-cv-00911, 2024 WL 4135626 (D. Utah Sept. 10, 2024); *NetChoice, LLC v. Fitch*, No. 24-cv-00170, 2024 WL 3276409 (S.D. Miss. July 1, 2024); *NetChoice, LLC v. Yost*, 716 F. Supp. 3d 539 (S.D. Ohio 2024); *NetChoice, LLC v. Griffin*, No. 23-cv-05105, 2023 WL 5660155 (W.D. Ark. Aug. 31, 2023); *Comput. & Commc’ns Indus. Ass’n et al. v. Paxton*, No. 24-cv-00849, 2024 WL 4051786 (W.D. Tex. Aug. 30, 2024).