



February 18, 2025

House Consumer & Public Affairs Committee
New Mexico State Capitol
490 Old Santa Fe Trail
Santa Fe, NM 87503

Re: HB 313 – "Digital Age Verification Act" (Oppose)

Dear Chair Ferrary and Members of the House Consumer & Public Affairs Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 313 in advance of the House Consumer & Public Affairs Committee hearing on February 18, 2025. 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 significantly impact 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

While CCIA shares the goal of increasing online safety, this bill would impose vague and ambiguous compliance burdens on businesses while jeopardizing consumer privacy.

Requirements under HB 313 are not administrable or well defined, creating serious compliance questions for both businesses and users and making minors less safe.

HB 313 contains vague, often undefined terms that would impose significant requirements and restrictions on application stores and covered manufacturers. For example, the obligation to "connect the developer of the application with the approving parent or guardian to facilitate supervision tools" is unclear and ambiguous, with none of those terms appearing elsewhere in the bill. Vague standards like "commercially reasonable and technically feasible steps" could also invite uncertainty and costly litigation over what is deemed "reasonable." The real-time data access requirement would undermine privacy and make children less safe, as developers

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/>.

would have access to sensitive personal information identifying an app store's users, including parents of their underage customers.

Currently available tools to conduct age determination are imperfect in estimating users' ages.

There is no perfect method of age determination, and the more data a method collects, the greater risk it poses to consumer privacy⁴ and small business sustainability.⁵ A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, contains more information regarding guiding principles for age assurance and how digital services have used such principles to develop best practices.⁶ The report found that “smaller companies may not be able to sustain their business” if forced to implement costly age verification methods, and that “[h]ighly accurate age assurance methods may depend on collection of new personal data such as facial imagery or government-issued ID.”⁷

Additionally, age verification software does not process all populations with equal accuracy. The National Institute of Standards and Technology (NIST) recently published a report evaluating six software-based age estimation and age verification tools that estimate a person's age based on the physical characteristics evident in a photo of their face.⁸ The report notes that facial age estimation accuracy is strongly influenced by algorithm, sex, image quality, region-of-birth, age itself, and interactions between those factors, with false positive rates generally being higher in women compared to men. CCIA encourages lawmakers to consider the current technological limitations in providing reliably accurate age estimation tools across all demographic groups.

Age verification and parental consent requirements raise significant privacy concerns.

The proposed bill suggests imposing a government-mandated requirement to verify all New Mexico users' ages that conflicts with data minimization principles ingrained in standard federal and international privacy and data protection compliance practices.⁹ Determining a user's age and obtaining parental consent inherently require collecting additional, sensitive data from those vulnerable users. If the state were to force companies to collect more user data even as others are requiring the collection of less data, it may place businesses in an

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>.

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 *Id.* at 10.

⁸ Kayee Hanaoka et al., *Face Analysis Technology Evaluation: Age Estimation and Verification (NIST IR 8525)*, National Institute of Standards and Technology (May 30, 2024), <https://doi.org/10.6028/NIST.IR.8525>.

⁹ 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/>.



untenable position of picking which state’s law to comply with, and which to unintentionally violate.¹⁰

Additionally, age verification solely at the device operating system or application store level overlooks access to websites via other means. Numerous applications are designed for use through a browser, which this method does not cover. While it might seem like a comprehensive solution to regulating access to certain content deemed undesirable for younger users, in reality, it falls short of achieving that goal.

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.¹¹ Though the intention to keep kids safe online is commendable, this bill is counterproductive to that initiative by requiring more data collection about young people.

Age verification 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 was struck down by the U.S. Supreme Court as unconstitutional because of the infeasibility.¹² After 25 years, age authentication still remains a vexing technical and social challenge.¹³

Recent state legislation that would implement online parental consent and age verification or estimation 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.¹⁴ CCIA anticipates that forthcoming rulings from the judiciary may be instructive in determining how, or whether, age determination requirements can be tied to granting user access to online speech. 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.

* * * * *

¹⁰ 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>.

¹¹ *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>.

¹² *Reno v. ACLU*, 521 U.S. 844, 855-57, 862 (1997).

¹³ 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>.

¹⁴ 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).



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,

Aodhan Downey
State Policy Manager, West
Computer & Communications Industry Association