CHAMBER OF PROGRESS

March 10, 2026

The Honorable Kriselda Valderrama
Chair
Committee on Economic Matters
Room 230, Taylor House Office Building
6 Bladen Street
Annapolis, MD 21401-1912

RE: Oppose HB 1179 - App Store Accountability Act

Dear Chair Valderrama and members of the Committee:

On behalf of Chamber of Progress, a tech industry association supporting public policies to build a society in which all people benefit from technological advances, **I respectfully urge you to oppose HB 1179,** which would mandate intrusive age verification and parental consent requirements that undermine privacy, centralize sensitive personal data, and risk cutting young people off from essential online resources.

HB 1179 requires intrusive age verification that undermines privacy for all users

HB 1179 requires app stores to perform account-level age verification using commercially available methods, effectively forcing the verification of the identity and age of all users, including adults. This approach necessitates the widespread collection, storage, and processing of sensitive personal information, such as government identification or biometric data, even when users are simply accessing lawful, general-purpose apps on their own devices.

For example, an adult downloading a weather app, a banking app, or a news app would be required to submit identifying information to an app store despite posing no child safety risk. This places adults in the unfair position of having to surrender sensitive personal data as a condition of participating in the digital economy, contradicting core principles of privacy, data minimization, and user autonomy.

There are a number of other concerns with mandating age verification. For example, strict age verification, which would require confirming a user's age without collecting additional personally identifiable information, is not technically feasible while still

respecting users' rights, privacy, and security.[1] This approach threatens online privacy for everyone.

Centralizing age verification at the app store level creates systemic security and misuse risks

By concentrating sensitive age and identity data at the app store level, the bill creates a single, high-value target for data breaches, misuse, and cyberattacks. App stores would be required to maintain large-scale repositories of verified identity information, increasing the potential harm if that data is compromised.

This risk is not hypothetical. Past breaches of centralized identity systems have exposed millions of users to fraud, identity theft, and harassment.For example, the 2017 Equifax breach compromised sensitive personal data, including Social Security numbers, for roughly 147 million Americans,[2] while a 2024 breach at National Public Data,[3] a background check and data broker company, potentially exposed up to 2.9 billion records containing sensitive personal information such as full names, addresses, and Social Security numbers.

Additionally, in Maryland, a breach at the Maryland Department of Labor exposed sensitive personal information, including Social Security numbers, for roughly 78,000 individuals whose records were stored in unemployment insurance and adult education program databases, illustrating the real-world consequences when centralized systems holding identity data are compromised.[4]

Under this framework, a single vulnerability at the app store level could expose sensitive information for vast numbers of users, including minors, magnifying the consequences of any failure.

HB 1179 shifts responsibility away from developers best positioned to implement tailored safety measures

---

[1] Sarah Forland et al. *Age Verification: The Complicated Effort to Protect Youth Online*. Open Technology Institute, New America, Apr. 22, 2024. https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/

[2] "Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach." Federal Trade Commission, Jul. 22, 2019. https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach

[3] Nicole Tan. "2.9 billion records may have been exposed in a data breach. Here's what to know." NBC Washington, Aug. 15, 2024. https://www.nbcwashington.com/news/national-international/2-9-billion-data-records-may-have-been-exposed-in-a-data-breach-heres-what-to-know/3695197/

[4] Lucas Ropek. "Maryland Grapples with Exposure of 78K Personal Records. Government Technology, Jul 8, 2019. https://www.govtech.com/security/maryland-grapples-with-exposure-of-78k-personal-records.html

App developers are generally better suited than app stores to design and implement safety features that reflect the specific risks, content, and use cases of their services. The bill instead shifts responsibility to the app store layer, requiring real-time transmission of users' age categories to developers and mandating uniform age-based restrictions.

For example, a social platform, an educational app, and a messaging service each present distinct safety considerations and already deploy different moderation tools, parental controls, and age-appropriate experiences. Imposing a one-size-fits-all model at the app store level risks weakening these platform-specific protections while relieving large services of accountability for how safety is actually implemented within their products.

Mandatory parental consent requirements risk harming teens in vulnerable or high-conflict households

HB 1179 requires minors to be linked to a verified parent account and mandates verifiable parental consent for every app download and in-app purchase. While parental involvement can be valuable, blanket consent requirements fail to account for family dynamics and can be misused in high-conflict or abusive households.

For example, teens seeking access to mental health resources, LGBTQ+ support communities, or educational tools could be blocked by a parent who is unsupportive or controlling. Research consistently shows that online engagement can reduce isolation and improve mental health outcomes for vulnerable youth, and policies that indiscriminately restrict access risk cutting off these critical lifelines.

HB 1179 prioritizes control over safety and risks unintended harm to young people

By emphasizing identity verification and parental control over flexible, context-specific safety measures, the bill risks substituting compliance for meaningful protection. Restricting access through rigid consent mechanisms does not address the underlying causes of online harm and may instead push young people toward less visible or less regulated online spaces.

A more effective approach would focus on empowering developers to build age-appropriate experiences, improving digital literacy, and providing families with tools that support safety without requiring universal identity verification or blanket parental permission for ordinary app use.

Recent Texas ruling highlights constitutional problems with app store age verification mandates

HB 1179 follows a policy path that courts are already rejecting. In December 2025, a federal judge blocked Texas's app store age verification law as likely unconstitutional under the First Amendment, finding that the state failed to use the least restrictive means to achieve its child safety goals and noting that existing parental control tools already allow families to manage children's app use without restricting lawful speech or requiring users to surrender identifying information.[5] HB 1179 adopts the same framework by requiring app stores to verify users' age categories and condition minors' app downloads and purchases on parental consent, relying on broad, account-level verification and default restrictions rather than targeted safety tools, and therefore raises the same legal and practical concerns that led the Texas law to be blocked before it could take effect.

Additionally, Utah is now facing a similar constitutional challenge. In February 2026, a lawsuit was filed seeking to block Utah's app store age verification law on First Amendment grounds, arguing that the state cannot require broad, account-level age gating and parental consent as a condition of accessing lawful apps.[6] This reinforces that courts are increasingly skeptical of app store age verification mandates as a constitutionally permissible approach to child safety.

For these reasons, **I respectfully urge you to oppose HB 1179.** While protecting young people online is a shared priority, this bill would erode privacy for all users, weaken platform-specific safety protections, and impose rigid consent requirements that risk harming vulnerable youth without meaningfully improving online safety.

Sincerely,

Brianna January
Director of State & Local Government Relations, Northeast US

[5] "Judge Blocks Texas's App Store Accountability Act as Unconstitutional Speech Restriction." Computer & Communications Industry Association, Dec. 23, 2025 https://ccianet.org/news/2025/12/judge-blocks-texass-app-store-accountability-act-as-unconstitutional-speech-restriction/; "CCIA Challenges Unconstitutional App Store Law in Utah." Computer & Communications Industry Association, Feb. 5, 2026. https://ccianet.org/news/2026/02/ccia-challenges-unconstitutional-app-store-law-in-utah/

[6] "CCIA Challenges Unconstitutional App Store Law in Utah." Computer & Communications Industry Association, Feb. 5, 2026. https://ccianet.org/news/2026/02/ccia-challenges-unconstitutional-app-store-law-in-utah/