DATE: March 6, 2026
TO: House Economic Matters Committee
FROM: The Entertainment Software Association
RE: HB 1179 – Oppose

Dear Chair Valderrama and Members of the House Economic Matters Committee,

On behalf of the Entertainment Software Association (ESA), which represents the leading publishers and developers of interactive entertainment in the United States, we write to share our concerns with House Bill 1179, which proposes mandatory age-verification and parental-consent requirements for mobile applications. While the goal of protecting children online and empowering parents is one that we all share, the approach outlined in HB 1179 risks creating significant unintended consequences for Maryland families, businesses, and the security of personal data.

Although well-intentioned, the bill's mandated age-verification framework would be difficult to implement in practice and would undermine existing parental control tools that already help families manage children's online experiences. Additionally, comparable legislation in Texas has been enjoined on First Amendment grounds. Related laws in Utah are currently facing legal challenges, and legislation in Louisiana is expected to undergo significant revisions before implementation. ESA outlines our concerns with HB 1179 below and urges the committee to consider alternative approaches to achieve the same goals, such as the California Digital Age Assurance Act.

Substantial Privacy and Data Security Risks

HB 1179 would require individuals to verify their age in order to use common mobile applications on phones or tablets including everyday services such as maps, weather, calculators, and music apps. This would necessitate the widespread collection, processing, storage, and transmission of highly sensitive personal information, including government-issued identification and potentially biometric data.

Even with safeguards, transmitting this information among app stores and developers would create serious risks by concentrating large volumes of sensitive data and linking personally identifiable information to virtually every user account—adult and minor alike.

Expanding data collection in this way runs counter to widely recognized best practices that encourage minimizing the amount of personal data companies collect and store. Increasing the number of entities required to handle sensitive identity data increases the likelihood of breaches, misuse, or unauthorized disclosure.

Conflicts with Existing Systems

For more than thirty years, the video game industry has developed and refined tools that allow parents to manage their children's online experiences directly.

HB 1179 would require app stores to collect age and parental consent information and transmit that data to developers, who must rely exclusively on those signals. This approach overlooks the fact that many companies already:

- Collect age information directly from users and parents
- Use legally recognized methods to obtain verifiable parental consent
- Tailor age-assurance processes to specific legal requirements and service designs

For example, the Federal Trade Commission has approved multiple mechanisms for obtaining verifiable parental consent under federal law. Companies often collect age information in different formats—such as date of birth, confirmation that a user is above a certain age threshold, or current age—depending on the service and the regulatory context.

Mandating reliance on a single third-party source of age information would override these carefully designed systems, even when those systems more accurately reflect parents' intent and satisfy compliance obligations.

Undermining Parental Choice and Flexibility

Today's video game platforms and digital services offer robust parental controls that allow families to tailor protections to their own needs. These tools commonly allow parents to:

- Set spending limits
- Restrict downloads based on age ratings
- Manage screen time and playtime
- Control communications and social features

These systems empower parents to establish flexible guardrails rather than requiring approval for every individual action. A rigid mandate that forces developers to rely solely on app-store-provided signals risks weakening these customizable safeguards and reducing parental autonomy.

Significant Compliance Burdens and Litigation Risk

HB 1179 would impose complex technical and operational requirements across both app stores and developers, creating substantial compliance burdens and legal uncertainty. Companies would face costly implementation challenges as well as exposure to enforcement actions and litigation.

Recent developments in other states illustrate these risks. Comparable legislation in Texas has been enjoined on First Amendment grounds. Related laws in Utah are currently facing legal challenges, and legislation in Louisiana is expected to undergo significant revisions before implementation.

These examples demonstrate that similar regulatory frameworks have not yet been successfully implemented in the United States.

Conclusion

Protecting children online is a critical priority, and the video game industry shares that goal. However, HB 1179's approach to age verification risks creating privacy harms, weakening existing parental tools, and imposing significant technical and legal burdens without clear evidence that it will improve safety outcomes.

A more effective path would be a flexible approach to age assurance—one that allows companies to obtain age information and parental consent directly from parents and users. Thank you for your consideration of these concerns and for your commitment to policies that both protect children and safeguard the privacy and security of Maryland residents.

Sincerely,

Jennifer Gibbons
VP, State Government Affairs
Entertainment Software Association