HB 1179 - Maryland App Store.pdf
Uploaded by: Chris McKenna
Position: FAV

March 6, 2026

Honorable Members of the Maryland
House Economic Matters Committee
230 Taylor House Office Building
Annapolis, Maryland 21401

We write in support of HB 1179, commonly referred to as the App Store Accountability Act, because it is a pragmatic, privacy-first, child-centric solution, utilizing existing technologies, to one of the most pressing challenges of our time: protecting children and families in an increasingly complex and exploitative digital world.

I lead Protect Young Eyes, a national digital wellness organization that advises legislators, schools, churches, and non-profits on the most effective techniques to protect children from online harm. Our activities include consulting with law enforcement (Internet Crimes Against Children officers), Children's Assessment Centers, and the world's largest technology organizations, sharing our expertise in parental controls, filters, and device set-up.

App stores serve as the central gatekeepers to how Maryland children interact on their devices, who use approximately 40 different apps per week. This unique position of App Stores makes them a natural and efficient doorway for implementing critical, commonsense protections, and for complying with basic contract law.

The strengths of HB 1179 include:

1. **Utilizing Existing Systems for Efficiency:** App stores **already collect** extensive user data, including age and family relationships, through features like Apple's Family Sharing and Google's Family Link. By building on these tools, the Act avoids adding complexity while maximizing effectiveness.
2. **Protecting Privacy Through Anonymized Data:** The Act mandates that age information shared with developers **remains anonymized**, safeguarding individual privacy. App Stores already share other types of anonymized data, like "Did you subscribe to the app?" with developers via API millions of times daily.
3. **Promoting Digital Wellness for all Maryland Children:** The Act allows developers to ***automatically*** enable safety-related features and defaults for **all Maryland minors**. Safety by default ensures *all* children receive the same protections. Not just those with parents with the ability and resources to navigate complex features.

Phone. 616.450.6719 **Email.** info@protectyoungeyes.com

The App Store Accountability Act is a secure, family-first, child-centric path forward. I suspect those who want access to your child's data won't like it. But that's where we're counting on the Maryland legislature to prevent trillion-dollar companies from signing contracts with your precious children.

If you visit Apple's App Store website, at the top it says: "**The apps you love. From a place you can trust.**"

In an era when digital harms to children are escalating, HB 1179 offers app stores an opportunity to fulfill their stated commitments to trust and safety. It sends a powerful message: that digital gatekeepers must take their responsibility to protect Maryland children and families as seriously as any brick-and-mortar institution would.

HB 1179 isn't asking app stores to do the job of parents. It's simply asking that they obey the law by receiving consent.

I ask for a do-pass on HB 1179. Thank you for your consideration.

Respectfully submitted,

Chris McKenna
Founder, CEO, Protect Young Eyes
President, The Better Tech Project

HB 1179_Digitial Childhood Alliance_Fav Written Te
Uploaded by: John Read
Position: FAV

Testimony of Digital Childhood Alliance
Before the Economic Matters Committee
Proponent Testimony on HB 1179

My name is John Read, and I am the Senior Policy Counsel for the Digital Childhood Alliance. The alliance consists of over 170 grassroots and larger organizations committed to protecting children and holding Big Tech accountable. Before joining the Digital Childhood Alliance, I was an attorney at the Department of Justice for 30 years, with my last years concentrated on legal issues surrounding Big Tech's businesses.

Today, 95% of all teens have access to a smartphone.[1] Teens spend an average of 7.5 hours per day on screens.[2] While on the phone, those teenagers are spending 88% of their time on apps, with the average teen receiving approximately 240 app notifications each day.[3]

Because teens vastly prefer an iPhone over an Android (88% versus 12%) and for brevity, I will focus on Apple's App Store, more than Google's.[4] Today you can download more than 1.9 million apps from almost 800,000 developers from the App Store.[5] Apple collects for itself and developers over $90 billion per year from those app downloads.[6] That has helped make Apple (and Google) two of the three wealthiest companies in the world, with market capitalizations above $3.7 trillion.[7]

With the growth of the iPhone and apps that run on it, there has been a spike in kids who are depressed, anxious, socially isolated, and contemplating suicide. Research shows that increased smartphone and app use is a major cause of that spike.[8] Even opponents recognize the problem and state that "children deserve a heightened level of

---

[1] https://www.pewresearch.org/internet/fact-sheet/teens-and-internet-device-access-fact-sheet/
[2] https://www.aacap.org/AACAP/Families_and_Youth/Facts_for_Families/FFF-Guide/Children-And-Watching-TV-054.aspx
[3] https://www.mobiloud.com/blog/what-percentage-of-internet-traffic-is-mobile; https://www.michiganmedicine.org/health-lab/study-average-teen-received-more-200-app-notifications-day
[4] https://mashable.com/article/teens-really-love-their-iphones (April 10, 2025)
[5] https://42matters.com/ios-apple-app-store-statistics-and-trends
[6] https://www.businessofapps.com/data/apple-app-store-statistics/ (January 22, 2025)
[7] https://companiesmarketcap.com/ (February 27, 2026)
[8] https://pmc.ncbi.nlm.nih.gov/articles/PMC7012622/ Canadian Medical Association Journal, "Smartphones, social media use and youth mental health" (2020); https://www.adventisthealth.org/blog/2023/august/how-screen-time-affects-teens-mental-health-and-/; https://www.psychiatrist.com/news/chronic-smartphone-use-linked-to-teen-anxiety-depression-and-insomnia/ ; Jonathan Haidt, *The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness* (2024).

security" online.[9] To address that issue, this bill gives parents more control over what apps their children download and use.

SB 372 focuses on the contracts that minors enter when they download apps onto their smartphone. SB 372 protects kids by ensuring parents are involved in that app contracting process.

When a consumer downloads an app, they agree to extensive terms of service which form a contract. While in the physical world minors cannot make contracts such as bank loans without permission of a parent or other responsible adult, Apple and Google operate differently in the digital world. Apple and Google facilitate a process where hundreds of millions of times a year unsophisticated minors contract away their rights to developers without any adult knowledge or approval.

These contracts often grant developers sweeping access to a minor's personal data, including location, contacts, and browsing history, all without a parent's consent. For example, Google's YouTube terms of service require minors to waive compensation for all their creative works they upload, while Google retains the rights to monetize the same content. Further, Google limits its liability for any damages its products cause the child. Google reduces the child's statute of limitation to one-year and unilaterally caps any damages at $500, regardless of how deeply it harmed a child.[10] To get around the fact that it is contracting with a minor, Google's terms of service says the minor "represent[s] that you have your parent or guardian's permission to use the Service."[11] SB 372 would make sure Google actually gets the parental permission it wants to claim the minor had.

Meta's terms of service grant it extensive rights over the minor's data.[12] Big Tech routinely tracks the engagement of minors with an app's content. They track the minor's precise location, voice recordings, browsing history, videos watched, and app activity across third-party sites. Developers then profit from their "free" apps by selling the minor's data. SB 372 gives parents who object to that the tools to prevent it.

A U.S. Senate Judiciary subcommittee hearing on September16, 2025, highlighted the problem with these terms of service. A minor was hospitalized because an AI chatbot app encouraged him to mutilate himself and hide it from his parents.[13] The boy currently requires constant medical care.

---

[9] TechNet March 6, 2026, opposition letter at 1.
[10] https://www.youtube.com/static?template=terms at "Limitation of Liability" section
[11] https://www.youtube.com/static?template=terms at "Permission by Parents or Guardian" section
[12] https://help.instagram.com/515230437301944 at "What Information do we collect?" section
[13] https://www.judiciary.senate.gov/imo/media/doc/e2e8fc50-a9ac-05ec-edd7-277cb0afcdf2/2025-09-16%20PM%20-%20Testimony%20-%20Doe.pdf

The family sued for help with the hospital bills and damages. That suit was held up because the minor, without parental consent, had accepted the app's terms of service which forced arbitration, and capped damages at $100. The tech company argued the minor's family could not sue but had to go to arbitration even to determine if its terms of service were valid.[14] SB 372 would solve this type of problem by statutorily voiding the unfair provisions in the terms of service, unless a parent consented to them.

Parents want to be involved. Surveys show that more than 80% of voters say parents should be empowered to consent to the contracts their children make and the apps they download.[15] Google's and Apple's app stores have unfortunately undermined those efforts for years. For example, up until a month ago, Google's policy, was to allow a 13-year-old to terminate any parental supervision of the child's apps without parental consent – even if the parent had earlier set up tools to approve what their child was downloading.[16] Only after pressure from child advocates and now that several states are consider bills like SB 372 has Google changed its policy to send both the parent and the 13-year-old an email letting them both know that the child can discontinue parental supervision.[17]

SB 372 empowers parents to protect minors from contracts and apps that are harmful. To make parental control meaningful, this bill requires developers to provide information on the contract terms and accurate age ratings so parents can have the information they need before consenting to an app for their child. Today, many developers falsely claim their apps are safe for children when they are not.[18]

Apple built its iPhone so that consumers can download apps only through its App Store.[19] That means Apple acts as a gatekeeper for the billions of apps downloaded from its app store each year. It also means the legislature can solve almost all the problem of minors entering app contracts without adult supervision by regulating just two entities – Apple's App Store and Google's Play Store – as opposed to asking the 800,000 developers to verify ages and obtain parental consent, most of whom do not have access to the data to do so.

---

[14] *Id*. at pp. 249-69

[15] https://alabamapolicy.org/2025/04/07/new-poll-finds-83-of-parents-favor-app-store-accountability/

[16] https://support.google.com/families/answer/7106787?hl=en (Copied in 2025)

[17] https://lifehacker.com/tech/google-is-changing-its-account-policy-about-minors-who-turn-13

[18] https://www.movieguide.org/news-articles/deceptive-age-ratings-appear-on-apple-app-store-report-finds.html

[19] The definition of App Store is appropriately limited to sites consumers use to *download* apps onto phones or tablets (*see* page 3, lines 8-11 & page 4 lines 3-9), something Apple allows only through the App Store. The definition does not cover gaming platforms or streaming services as some opponents fear.

This bill protects privacy – especially children's. Apple already knows and can verify its customer's age. The bill would require developers to protect any age-related data they obtain. Privacy is also improved for minors because now parents can reject any apps that through the terms of service permit the developer to obtain and sell a teenager's data.[20]

The Act does not burden adults with age verification. A consumer's age is already in their phone, and most adults already have a credit card in their digital wallet (which provides all the information needed to verify that someone is an adult). Consumers entered their age when they registered their device and got access to the app store. Apple has already created the APIs to send anonymous age category signals to developers for foreign markets and those states that have passed App Store legislation.[21] With the App Store Accountability Act, age verification is seamless for adults – no app developer will need to individually bother an adult for age verification because the app store will have already handled it in a way that protects privacy.

The bill does not unduly expose small developers to litigation risks. In fact, it has a safe harbor for developers that rely in good faith on the app store's age verification process and the signal indicating the store obtained parental consent for the minor.[22]

The Act is specifically designed to comply with the First Amendment by applying to all apps, not some subset (which could arguably raise First Amendment concerns about preferential treatment). In this way, SB 372 is different from what recently happened in Texas. In Texas, a trial judge found that app store law discriminated among apps because it excepted pre-downloaded apps, apps used for standardized testing for colleges, and emergency service apps like 911. As a result, that judge failed the Texas law under the strict scrutiny standard.[23] That decision has been appealed, but regardless of its outcome, SB 372 is different from the Texas law because it does not except those three types of apps and therefore would not warrant the same result.

In contrast, SB 372 applies to all apps, demonstrating that the legislation is "directed at unlawful conduct having nothing to do with . . . the expressive activity."[24] By applying to all apps, SB 372 is akin to the regulation the Supreme Court held did not violate

---

[20] The federal Children's Online Privacy Protection Act does not prohibit developers from selling the data of teenagers.

[21] https://techcrunch.com/2026/02/24/apple-rolls-out-age-verification-tools-worldwide-to-comply-with-growing-web-of-child-safety-laws/

[22] *See* section 14-5106(A) & (B)

[23] See Order of December 23, 2025, *Computer & Communications Industry Assoc. v. Paxton*, 1:25-CV-1660-RP (W.D. Texas)

[24] *Arcara v. Cloud Books, Inc.,* 478 U.S. 697, 707 (1986).

the First Amendment because it did not "single out any topic or subject matter for different treatment."[25]

I wholeheartedly support SB 372.

[25] *City of Austin, Texas v. Reagan National Advertising of Austin, LLC*, 596 U.S. 61, 71 (2022).

hb 1179 apps Nkongolo.pdf
Uploaded by: Peggy Cairns
Position: FAV

HOUSE BILL 1179

I3, I4 6lr1320

By: **Delegates Nkongolo, Arentz, Hornberger, Miller, and Tomlinson**
Introduced and read first time: February 11, 2026
Assigned to: Economic Matters

A BILL ENTITLED

AN ACT concerning

Consumer Protection – Application Store Accountability Act

FOR the purpose of establishing requirements for application store providers and developers; creating requirements for age verification and parental consent; prohibiting application store providers and developers from enforcing certain contracts under certain circumstances; prohibiting application store providers and developers from misrepresenting certain parental consent disclosures; authorizing the Consumer Protection Division in the Office of the Attorney General to adopt certain rules; making a violation of this Act an unfair, abusive, or deceptive trade practice that is subject to enforcement and penalties under the Maryland Consumer Protection Act; and generally relating to application store accountability.

BY repealing and reenacting, with amendments,
Article – Commercial Law
Section 13–301(14)(xlvii)
Annotated Code of Maryland
(2025 Replacement Volume)

BY repealing and reenacting, without amendments,
Article – Commercial Law
Section 13–301(14)(xlviii)
Annotated Code of Maryland
(2025 Replacement Volume)

BY adding to
Article – Commercial Law
Section 13–301(14)(xlix); and 14–5101 through 14–5107 to be under the new subtitle "Subtitle 51. Application Store Accountability Act"
Annotated Code of Maryland
(2025 Replacement Volume)

EXPLANATION: **CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.**
[Brackets**]** indicate matter deleted from existing law.

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That the Laws of Maryland read as follows:

Article – Commercial Law

13–301.

Unfair, abusive, or deceptive trade practices include any:

(14) Violation of a provision of:

(xlvii) Title 14, Subtitle 50 of this article; **[**or**]**

(xlviii) Section 13–411.1(c)(2) of the Transportation Article; or

(XLIX) TITLE 14, SUBTITLE 51 OF THIS ARTICLE; OR

SUBTITLE 51. APPLICATION STORE ACCOUNTABILITY ACT.

14–5101.

(A) IN THIS SUBTITLE THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.

(B) "ACCOUNT HOLDER" MEANS AN INDIVIDUAL WHO IS ASSOCIATED WITH A MOBILE DEVICE.

(C) (1) "AGE CATEGORY" MEANS A CATEGORY BASED ON A RANGE OF USER AGES.

(2) "AGE CATEGORY" INCLUDES:

(I) CHILD;

(II) YOUNGER TEENAGER;

(III) OLDER TEENAGER; AND

(IV) ADULT.

(D) "AGE CATEGORY DATA" MEANS INFORMATION ABOUT AN ACCOUNT HOLDER'S AGE CATEGORY THAT IS COLLECTED BY AN APPLICATION STORE PROVIDER AND IS SHARED WITH A DEVELOPER.

(E) "AGE RATING" MEANS ONE OR MORE CLASSIFICATIONS THAT ASSESS THE SUITABILITY OF AN APPLICATION'S CONTENT AND FUNCTIONS FOR DIFFERENT AGE GROUPS.

(F) (1) "APPLICATION" MEANS A SOFTWARE APPLICATION OR AN ELECTRONIC SERVICE THAT A USER MAY RUN OR DIRECT ON A MOBILE DEVICE.

(2) "APPLICATION" INCLUDES A PRE–INSTALLED APPLICATION ON A MOBILE DEVICE.

(G) "APPLICATION STORE" MEANS A PUBLICLY AVAILABLE WEBSITE, SOFTWARE APPLICATION, OR ELECTRONIC SERVICE THAT ALLOWS ACCOUNT HOLDERS TO DOWNLOAD APPLICATIONS FROM THIRD–PARTY DEVELOPERS ONTO A MOBILE DEVICE.

(H) "APPLICATION STORE PROVIDER" MEANS A PERSON THAT OWNS, OPERATES, OR CONTROLS AN APPLICATION STORE THAT ALLOWS ACCOUNT HOLDERS IN THE STATE TO DOWNLOAD APPLICATIONS ONTO A MOBILE DEVICE.

(I) "CHILD" MEANS AN INDIVIDUAL WHO IS UNDER 13 YEARS OLD.

(J) "CONTENT DESCRIPTION" MEANS A DESCRIPTION OF THE SPECIFIC CONTENT ELEMENTS OR FUNCTIONS THAT INFORMED AN APPLICATION'S AGE RATING.

(K) "DEVELOPER" MEANS A PERSON THAT OWNS OR CONTROLS A PRE–INSTALLED APPLICATION ON A MOBILE DEVICE OR AN APPLICATION MADE AVAILABLE THROUGH AN APPLICATION STORE IN THE STATE.

(L) "DIVISION" MEANS THE DIVISION OF CONSUMER PROTECTION OF THE OFFICE OF THE ATTORNEY GENERAL.

(M) "KNOWINGLY" MEANS TO ACT WITH ACTUAL KNOWLEDGE OR TO ACT WITH KNOWLEDGE FAIRLY INFERRED BASED ON OBJECTIVE CIRCUMSTANCES.

(N) (1) "MINOR" MEANS, EXCEPT AS PROVIDED IN PARAGRAPH (2) OF THIS SUBSECTION, A PERSON UNDER THE AGE OF 18 YEARS.

(2) "MINOR" DOES NOT INCLUDE AN INDIVIDUAL UNDER THE AGE OF 18 YEARS WHO IS MARRIED OR LEGALLY EMANCIPATED.

(O) "MINOR ACCOUNT" MEANS AN ACCOUNT WITH AN APPLICATION STORE PROVIDER THAT:

(1) IS ESTABLISHED BY A PERSON FOR THE BENEFIT OF A MINOR; AND

(2) IS ASSOCIATED WITH A PARENT ACCOUNT.

(P) "MOBILE DEVICE" MEANS A PHONE OR GENERAL PURPOSE TABLET THAT:

(1) PROVIDES CELLULAR OR WIRELESS CONNECTIVITY;

(2) IS CAPABLE OF CONNECTING TO THE INTERNET;

(3) RUNS A MOBILE OPERATING SYSTEM; AND

(4) IS CAPABLE OF RUNNING APPLICATIONS THROUGH A MOBILE OPERATING SYSTEM.

(Q) "MOBILE OPERATING SYSTEM" MEANS SOFTWARE THAT:

(1) MANAGES MOBILE DEVICE HARDWARE RESOURCES;

(2) PROVIDES COMMON SERVICES FOR MOBILE DEVICE PROGRAMS;

(3) CONTROLS MEMORY ALLOCATION; AND

(4) PROVIDES INTERFACES FOR APPLICATIONS TO ACCESS DEVICE FUNCTIONALITY.

(R) "OLDER TEENAGER" MEANS A PERSON WHO IS AT LEAST 16 YEARS OLD AND UNDER THE AGE OF 18 YEARS.

(S) "PARENT" MEANS A PERSON WHO IS REASONABLY BELIEVED TO BE A PARENT, A LEGAL GUARDIAN, A PERSON WITH LEGAL CUSTODY, OR ANY OTHER PERSON WHO HAS THE LEGAL AUTHORITY TO MAKE DECISIONS ON BEHALF OF A MINOR UNDER STATE LAW.

(T) "PARENT ACCOUNT" MEANS AN ACCOUNT WITH AN APPLICATION STORE PROVIDER THAT:

(1) IS VERIFIED AS ESTABLISHED BY A PERSON WHO THE APPLICATION STORE PROVIDER HAS DETERMINED IS NOT A MINOR THROUGH THE APPLICATION STORE PROVIDER'S AGE VERIFICATION METHODS; AND

(2) MAY BE AFFILIATED WITH ONE OR MORE MINOR ACCOUNTS.

(U) "PARENTAL CONSENT DISCLOSURE" MEANS INFORMATION PROVIDED BY AN APPLICATION STORE PROVIDER THAT INCLUDES:

(1) IF THE APPLICATION STORE PROVIDER HAS AN AGE RATING FOR AN APPLICATION OR IN–APPLICATION PURCHASE, THE AGE RATING FOR THE APPLICATION OR IN–APPLICATION PURCHASE;

(2) IF THE APPLICATION STORE PROVIDER HAS A CONTENT DESCRIPTION FOR AN APPLICATION OR IN–APPLICATION PURCHASE, THE CONTENT DESCRIPTION FOR THE APPLICATION OR IN–APPLICATION PURCHASE;

(3) A DESCRIPTION OF:

(I) THE PERSONAL DATA COLLECTED BY THE APPLICATION FROM AN ACCOUNT HOLDER; AND

(II) THE PERSONAL DATA SHARED BY THE APPLICATION WITH A THIRD PARTY; AND

(III) THE METHODS IMPLEMENTED BY THE DEVELOPER TO PROTECT THE PERSONAL DATA THAT IS COLLECTED.

(V) (1) "PRE–INSTALLED APPLICATION" MEANS AN APPLICATION, OR PORTION OF AN APPLICATION, THAT HAS BEEN INSTALLED OR PARTIALLY INSTALLED ON A MOBILE DEVICE BEFORE THE CONSUMER USES THE MOBILE DEVICE FOR THE FIRST TIME, INCLUDING WEB BROWSERS, SEARCH ENGINES, AND MESSAGING APPLICATIONS.

(2) "PRE–INSTALLED APPLICATION" DOES NOT INCLUDE AN APPLICATION THAT IS A DEVICE DRIVER OR THAT ALLOWS A MOBILE DEVICE TO PERFORM CORE OPERATIONS IN ORDER TO FUNCTION AS INTENDED.

(W) "SIGNIFICANT CHANGE" MEANS A MODIFICATION TO THE TERMS OF SERVICE OR PRIVACY POLICY FOR AN APPLICATION THAT:

(1) MATERIALLY ALTERS THE CATEGORIES OF DATA COLLECTED, STORED, OR SHARED;

(2) MATERIALLY ALTERS THE APPLICATION'S AGE RATING OR CONTENT DESCRIPTIONS; OR

(3) INTRODUCES, WHERE NO IN–APPLICATION PURCHASES WERE PREVIOUSLY PRESENT:

(I) IN–APPLICATION PURCHASES; OR

(II) ADVERTISEMENTS.

(X) "VERIFIABLE PARENTAL CONSENT" MEANS AUTHORIZATION THAT:

(1) IS PROVIDED BY A PARENT ACCOUNT;

(2) IS GIVEN AFTER AN APPLICATION STORE PROVIDER HAS CLEARLY AND CONSPICUOUSLY PROVIDED THE PARENTAL CONSENT DISCLOSURE AS PART OF THE APPLICATION DOWNLOAD, PURCHASE, OR IN–APPLICATION PURCHASE PROCESS; AND

(3) REQUIRES THE PARENT TO MAKE AN AFFIRMATIVE CHOICE TO:

(I) GRANT CONSENT; OR

(II) DECLINE CONSENT.

(Y) "YOUNGER TEENAGER" MEANS AN INDIVIDUAL WHO IS AT LEAST 13 YEARS OLD AND YOUNGER THAN 16 YEARS OLD.

14–5102.

(A) AT THE TIME AN INDIVIDUAL CREATES AN ACCOUNT, AN APPLICATION STORE PROVIDER SHALL:

(1) REQUEST AGE CATEGORY INFORMATION FROM THE INDIVIDUAL; AND

(2) VERIFY THE INDIVIDUAL'S AGE CATEGORY USING:

(I) COMMERCIALLY AVAILABLE METHODS THAT ARE REASONABLY DESIGNED TO ENSURE ACCURACY; OR

(II) AN AGE VERIFICATION METHOD OR PROCESS THAT COMPLIES WITH REGULATIONS ADOPTED BY THE DIVISION UNDER § 14–5104 OF THIS SUBTITLE.

(B) FOR AN ACCOUNT IN EXISTENCE BEFORE OCTOBER 1, 2026, AN APPLICATION STORE PROVIDER SHALL, ON OR BEFORE OCTOBER 1, 2027:

(1) REQUEST AGE CATEGORY INFORMATION FROM THE INDIVIDUAL; AND

(2) VERIFY THE AGE CATEGORY OF THE INDIVIDUAL USING:

(I) COMMERCIALLY AVAILABLE METHODS THAT ARE REASONABLY DESIGNED TO ENSURE ACCURACY; OR

(II) AN AGE VERIFICATION METHOD OR PROCESS THAT COMPLIES WITH REGULATIONS ADOPTED BY THE DIVISION UNDER § 14–5104 OF THIS SUBTITLE.

(C) IF THE APPLICATION STORE PROVIDER DETERMINES THE INDIVIDUAL IS A MINOR, THE PROVIDER SHALL:

(1) REQUIRE THE ACCOUNT TO BE AFFILIATED WITH A PARENT ACCOUNT;

(2) OBTAIN VERIFIABLE PARENTAL CONSENT FROM THE HOLDER OF THE AFFILIATED PARENT ACCOUNT EACH TIME BEFORE ALLOWING THE MINOR TO:

(I) DOWNLOAD AN APPLICATION;

(II) PURCHASE AN APPLICATION; OR

(III) MAKE AN IN–APPLICATION PURCHASE;

(3) AFTER RECEIVING NOTICE OF A SIGNIFICANT CHANGE FROM A DEVELOPER:

(I) NOTIFY THE ACCOUNT HOLDER OF THE SIGNIFICANT CHANGE; AND

(II) FOR A MINOR ACCOUNT:

1. NOTIFY THE PARENT ACCOUNT HOLDER; AND

2. OBTAIN RENEWED VERIFIABLE PARENTAL CONSENT BEFORE PROVIDING ACCESS TO THE SIGNIFICANTLY CHANGED VERSION;

(4) PROVIDE THE FOLLOWING INFORMATION TO A DEVELOPER, IN RESPONSE TO A REQUEST AUTHORIZED UNDER § 14–5103 OF THIS SUBTITLE:

(I) AGE CATEGORY DATA FOR AN ACCOUNT HOLDER; AND

(II) THE STATUS OF VERIFIABLE PARENTAL CONSENT FOR A MINOR;

(5) PROVIDE A METHOD FOR A PARENT ACCOUNT HOLDER TO WITHDRAW CONSENT AND NOTIFY A DEVELOPER WHEN THE PARENT REVOKES VERIFIABLE PARENTAL CONSENT; AND

(6) PROTECT AGE CATEGORY DATA AND ANY ASSOCIATED VERIFICATION DATA BY:

(I) LIMITING COLLECTION AND PROCESSING TO DATA NECESSARY FOR:

1. VERIFYING AN ACCOUNT HOLDER'S AGE CATEGORY;

2. OBTAINING VERIFIABLE PARENTAL CONSENT; OR

3. MAINTAINING COMPLIANCE RECORDS; AND

(II) TRANSMITTING AGE CATEGORY DATA USING INDUSTRY–STANDARD ENCRYPTION PROTOCOLS THAT ENSURE DATA INTEGRITY AND DATA CONFIDENTIALITY; AND

(III) FOR A PRE–INSTALLED APPLICATION, IN RESPONSE TO A REQUEST FROM A DEVELOPER;

1. PROVIDING AVAILABLE AGE CATEGORY INFORMATION; AND

2. TAKING REASONABLE MEASURES TO FACILITATE VERIFIABLE PARENTAL CONSENT FOR USE OF THE APPLICATION.

(D) AN APPLICATION STORE PROVIDER MAY NOT:

(1) ENFORCE A CONTRACT OR TERMS OF SERVICE AGAINST A MINOR UNLESS THE APPLICATION STORE PROVIDER HAS OBTAINED VERIFIABLE PARENTAL CONSENT;

(2) KNOWINGLY MISREPRESENT THE INFORMATION IN THE PARENTAL CONSENT DISCLOSURE; OR

(3) SHARE AGE CATEGORY DATA AND ANY ASSOCIATED DATA EXCEPT AS REQUIRED BY THIS SUBTITLE OR OTHERWISE REQUIRED BY LAW.

14–5103.

(A) A DEVELOPER SHALL:

(1) VERIFY THROUGH THE APPLICATION STORE'S DATA–SHARING METHODS:

(I) THE AGE CATEGORY DATA OF ACCOUNT HOLDERS; AND

(II) FOR A MINOR'S ACCOUNT, WHETHER VERIFIABLE PARENTAL CONSENT HAS BEEN OBTAINED;

(2) NOTIFY APPLICATION STORE PROVIDERS OF A SIGNIFICANT CHANGE TO AN APPLICATION;

(3) USE AGE CATEGORY DATA RECEIVED THROUGH THE APPLICATION STORE'S DATA–SHARING METHODS TO:

(I) ENFORCE ANY DEVELOPER–CREATED AGE–RELATED RESTRICTIONS, SAFETY–RELATED FEATURES, OR DEFAULTS; AND

(II) ENSURE COMPLIANCE WITH APPLICABLE LAWS AND REGULATIONS; AND

(4) REQUEST AGE CATEGORY DATA OR VERIFIABLE PARENTAL CONSENT:

(I) AT THE TIME AN ACCOUNT HOLDER:

1. DOWNLOADS AN APPLICATION;

2. PURCHASES AN APPLICATION; OR

3. LAUNCHES A PRE–INSTALLED APPLICATION FOR THE FIRST TIME;

(II) WHEN IMPLEMENTING A SIGNIFICANT CHANGE TO THE APPLICATION; OR

(III) TO COMPLY WITH APPLICABLE LAW.

(B) A DEVELOPER MAY REQUEST AGE CATEGORY DATA:

(1) NOT MORE THAN ONCE DURING EACH 12–MONTH PERIOD TO VERIFY:

(I) THE ACCURACY OF AGE CATEGORY DATA ASSOCIATED WITH AN ACCOUNT HOLDER; OR

(II) CONTINUED ACCOUNT USE WITHIN THE AGE CATEGORY;

(2) WHEN THERE IS REASONABLE SUSPICION OF:

(I) ACCOUNT TRANSFER; OR

(II) MISUSE OUTSIDE THE AGE CATEGORY; OR

(3) AT THE TIME AN ACCOUNT HOLDER CREATES A NEW ACCOUNT WITH THE DEVELOPER.

(C) WHEN IMPLEMENTING ANY DEVELOPER–CREATED AGE–RELATED RESTRICTIONS, SAFETY–RELATED FEATURES, OR DEFAULTS, A DEVELOPER SHALL USE THE LOWEST AGE CATEGORY INDICATED BY:

(1) AGE CATEGORY DATA RECEIVED THROUGH THE APPLICATION STORE'S DATA–SHARING METHODS; OR

(2) AGE DATA INDEPENDENTLY COLLECTED BY THE DEVELOPER.

(D) A DEVELOPER MAY NOT:

(1) ENFORCE A CONTRACT OR TERMS OF SERVICE AGAINST A MINOR UNLESS THE DEVELOPER HAS VERIFIED THROUGH AN APPLICATION STORE'S DATA–SHARING METHODS THAT VERIFIABLE PARENTAL CONSENT HAS BEEN OBTAINED;

(2) KNOWINGLY MISREPRESENT ANY INFORMATION IN THE PARENTAL CONSENT DISCLOSURE; OR

(3) SHARE AGE CATEGORY DATA WITH ANY PERSON.

14–5104.

THE DIVISION SHALL ADOPT REGULATIONS ESTABLISHING PROCESSES AND MEANS BY WHICH AN APPLICATION STORE PROVIDER MAY VERIFY AN ACCOUNT HOLDER'S AGE CATEGORY IN ACCORDANCE WITH § 14–5102(A) OF THIS SUBTITLE.

14–5105.

(A) A VIOLATION OF THIS SUBTITLE IS:

(1) AN UNFAIR, ABUSIVE, OR DECEPTIVE TRADE PRACTICE WITHIN THE MEANING OF TITLE 13 OF THIS ARTICLE; AND

(2) SUBJECT TO THE ENFORCEMENT AND PENALTY PROVISIONS CONTAINED IN TITLE 13 OF THIS ARTICLE, EXCEPT FOR § 13–411 OF THIS ARTICLE.

(B) IN ADDITION TO REMEDIES PROVIDED UNDER TITLE 13 OF THIS ARTICLE, THE ATTORNEY GENERAL MAY BRING AN ACTION AGAINST AN APPLICATION STORE PROVIDER OR A DEVELOPER TO RECOVER A CIVIL PENALTY NOT TO EXCEED $7,500 FOR EACH VIOLATION.

(C) IF A MINOR WAS HARMED BY A VIOLATION OF THIS SUBTITLE, THE COURT SHALL AWARD A PREVAILING PLAINTIFF:

(1) REMEDIES PROVIDED UNDER TITLE 13 OF THIS ARTICLE;

(2) THE GREATER OF ACTUAL DAMAGES OR $1,000 FOR EACH VIOLATION; AND

(3) PUNITIVE DAMAGES IF THE VIOLATION WAS EGREGIOUS.

14–5106.

(A) A DEVELOPER IS NOT LIABLE FOR A VIOLATION OF THIS SUBTITLE IF THE DEVELOPER DEMONSTRATES THAT THE DEVELOPER:

(1) RELIED IN GOOD FAITH ON APPLICABLE AGE CATEGORY DATA RECEIVED THROUGH AN APPLICATION STORE'S DATA–SHARING METHODS;

(2) RELIED IN GOOD FAITH ON NOTIFICATION FROM AN APPLICATION STORE PROVIDER THAT VERIFIABLE PARENTAL CONSENT WAS OBTAINED IF THE ACCOUNT HOLDER WAS A MINOR; AND

(3) COMPLIED WITH THE REQUIREMENTS DESCRIBED IN § 14–5103 OF THIS SUBTITLE.

(B) A DEVELOPER IS NOT LIABLE FOR A VIOLATION IN DETERMINING AN APPLICATION'S AGE RATING AND CONTENT DESCRIPTION FOR PURPOSES OF § 14–5103(D)(2) OF THIS SUBTITLE IF THE DEVELOPER:

(1) USES WIDELY ADOPTED INDUSTRY STANDARDS TO DETERMINE THE APPLICATION'S AGE CATEGORY AND CONTENT DESCRIPTION; AND

(2) APPLIES THOSE STANDARDS CONSISTENTLY AND IN GOOD FAITH.

(C) THE PROVISIONS OF SUBSECTIONS (A) AND (B) OF THIS SECTION:

(1) APPLY ONLY TO ACTIONS BROUGHT UNDER THIS SUBTITLE; AND

(2) DO NOT LIMIT THE LIABILITY OF A DEVELOPER OR AN APPLICATION STORE UNDER ANY OTHER APPLICABLE LAW.

(D) NOTHING IN THIS SUBTITLE MAY BE CONSTRUED AS LIMITING OR NEGATING ANY OTHER AVAILABLE REMEDIES OR RIGHTS AUTHORIZED UNDER THE LAWS OF THE STATE OR THE UNITED STATES.

14–5107.

THIS SUBTITLE MAY NOT BE CONSTRUED TO:

(1) PREVENT AN APPLICATION STORE PROVIDER OR A DEVELOPER FROM TAKING REASONABLE MEASURES TO:

(I) BLOCK, DETECT, OR PREVENT DISTRIBUTION TO MINORS OF:

1. UNLAWFUL MATERIAL;

2. OBSCENE MATERIAL; OR

3. OTHER HARMFUL MATERIAL;

(II) BLOCK OR FILTER SPAM;

(III) PREVENT CRIMINAL ACTIVITY; OR

(IV) PROTECT THE APPLICATION STORE OR APPLICATION SECURITY;

(2) REQUIRE AN APPLICATION STORE PROVIDER TO DISCLOSE USER INFORMATION TO A DEVELOPER BEYOND AGE CATEGORY DATA OR STATUS OF VERIFIABLE PARENTAL CONSENT;

(3) ALLOW AN APPLICATION STORE PROVIDER OR A DEVELOPER TO IMPLEMENT MEASURES REQUIRED UNDER THIS SUBTITLE IN A MANNER THAT IS ARBITRARY, CAPRICIOUS, ANTICOMPETITIVE, OR UNLAWFUL;

(4) REQUIRE AN APPLICATION STORE PROVIDER OR DEVELOPER TO BLOCK ACCESS TO AN APPLICATION THAT AN ACCOUNT HOLDER HAS DOWNLOADED OR INSTALLED ONTO A MOBILE DEVICE, EXCEPT WHEN:

(I) A PARENT ACCOUNT HOLDER REVOKES VERIFIABLE CONSENT FOR AN AFFILIATED MINOR ACCOUNT; OR

(II) THERE IS A SIGNIFICANT CHANGE TO THE APPLICATION;

(5) REQUIRE A DEVELOPER TO COLLECT, RETAIN, RE–IDENTIFY, OR LINK ANY INFORMATION BEYOND THAT WHICH IS:

(I) NECESSARY TO VERIFY AGE CATEGORY DATA AS REQUIRED BY THIS SUBTITLE; AND

(II) COLLECTED, RETAINED, RE–IDENTIFIED, OR LINKED IN THE DEVELOPER'S ORDINARY COURSE OF BUSINESS; OR

(6) RELIEVE A DEVELOPER OF THE DEVELOPER'S OBLIGATION TO CONDUCT AGE VERIFICATION AS OTHERWISE REQUIRED BY LAW, EXCEPT THAT A DEVELOPER MAY RELY ON AGE CATEGORY DATA OBTAINED UNDER THIS SUBTITLE IF THE AGE CATEGORY DATA SATISFIES THE REQUIREMENTS OF APPLICABLE LAW.

SECTION 2. AND BE IT FURTHER ENACTED, That, if any provision of this Act or the application of any provision of this Act to any person or circumstance is held invalid for any reason in a court of competent jurisdiction, the invalidity does not affect other provisions or any other application of this Act that can be given effect without the invalid provision or application, and for this purpose the provisions of this Act are declared severable.

SECTION 3. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2026.

MD_LetterinSupport_H.B.1179_ApplicationStoreAccoun

Uploaded by: Sarah Thacker

Position: FAV

NATIONAL CENTER ON SEXUAL EXPLOITATION

Established 1962

Written Testimony of Sarah Thacker, Legislative Analyst
National Center on Sexual Exploitation
1201 F St NW, Washington, D.C. 20004

Testimony in Favor of MD H.B. 1179, Consumer Protection – App Store Accountability Act
Maryland General Assembly, Economic Matters Committee
March 10, 2026

Chairwoman Valderrama, Vice Chair Charkoudian, and Members of the Committee,

My name is Sarah Thacker. I am a lifelong resident of Southern Maryland, and a Legislative Analyst for the the National Center on Sexual Exploitation, an organization with a mission to eradicate all forms of sexual exploitation and abuse. I urge you to support HB 1179, a strategic solution to protect children from exposure to harmful content online.

As our world has become increasingly digital, the dangers facing children have followed suit. Today, nearly 95% of teenagers report having access to a cellphone, and predators are well aware of this. Worse still, these devices and the apps on them are designed to be addictive, engineered to capture attention, and optimized to maintain young users' attention for as long as possible. As a substitute teacher and math coach, I have walked into classrooms at every level in Maryland where students are at their desk, wearing headphones, and on a laptop for hours. Just last Friday I spoke with a class of 27 fifth graders, where every single student had at least two devices in their possession.

Whistleblower testimony and internal company documents have revealed that major tech platforms consistently prioritize profit over child safety, despite clear evidence of harm. Big Tech companies cannot be trusted to self-regulate. Use of these platforms exposes children to a growing array of harms, including addiction, depression, loneliness, anxiety, dissatisfaction with life, self-harm, eating disorders, cyberbullying, sex-trafficking, exposure to child sexual abuse material, suicide, and more.

Unfortunately, these harms are ever-present in Maryland. In that same fifth grade class, at least half reported that they have experienced a dangerous interaction on their device while teachers report that parents consistently reach out to them regarding concerning online interactions.

Research shows that approximately 90% of digital activity occurs within apps, making app stores the primary gatekeepers controlling access to digital content–and the harms Maryland kids are experiencing online. Yet, app stores currently bear little responsibility for preventing children from these experiences. Descriptions of apps are often inaccurate–designed to mislead parents–and age ratings are assigned by developers seeking to sell products, regardless of rating accuracy.

For example, the apps Instagram and Snapchat consistently appear on Bark's list of dangerous apps in terms of severe bullying, severe violence, depression, body image concerns, and suicidal ideation. Yet Instagram is currently rated appropriate for kids ages 12+ and SNAP's current age rating is 13+. These age assignments should not be in the hands of those selling the product but should be verified by external experts in order to guard against potential harm.

The App Store Accountability Act addresses this gap by placing responsibility where it belongs: on the app store. This approach mirrors other industries, where retailers are responsible for verifying a consumer's age before selling dangerous products. The digital marketplace should be no different.

The bill also prevents corporations from entering into contracts with children without parental consent. Every day, app stores facilitate contracts between minors and billion-dollar companies which routinely give companies access to a child's personal data, exact location, camera, microphone, and more. This would not be permitted in every other industry.

For far too long, Big Tech has operated with a special exemption from the rules that apply to everyone else. This bill rightly corrects this imbalance. Maryland has the opportunity to protect children, empowers parents, and hold powerful corporations accountable.

Thank you for your attention and consideration.

Chamber of Progress_MD HB 1179_Oppose.pdf
Uploaded by: Brianna January
Position: UNF

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/

2026-06-03-TPA Written Testimony Against MDHB1179.
Uploaded by: David McGarry
Position: UNF

TAXPAYERS PROTECTION ALLIANCE

March 6, 2026

Maryland House of Delegates
Economic Matters Committee
6 Bladen Street, House Office Building, Room 230
Annapolis, MD 21401

Dear Chair Valderrama, Vice Chair Charkoudian and Members of the Committee:

On behalf of the millions of taxpayers and consumers we represent, the Taxpayers Protection Alliance (TPA) writes to express its concerns with House Bill 1179, a bill relating to app stores and age verification. Despite its noble desire to protect children in the digital age, HB1179 would in fact do the opposite. This misguided legislation would endanger the privacy and data security of children and families across the state.

HB1179's fundamental flaw is its requirement that users of app stores—the gatekeepers of the digital world—submit to age verification. Age verification requires users to submit a significant amount of sensitive personal information, which then becomes stored in large databases, liable to be hacked or to fall victim to data breaches. This information usually takes the form of scans of government-issued identification documents or biometric data, such as facial scans. Given regular cybersecurity lapses, this mass collection of sensitive data would directly undermine the goal of ensuring children's safety in the digital world.

Children already face vast privacy dangers spurred by cybercrime. As noted by the R Street Institute last year, "The problem is so extensive that research by Experian suggests that 25 percent of children will be victims of identity fraud or theft by the time they are 18."[1] Moreover, R Street continues, "More than half of minors who were victims of identity theft report being denied access to credit at least once because of it, and some deal with the consequences for a decade or more. Some have even acquired a lifelong criminal record for an offense committed by the thief that stole their identity." Requiring children to provide sensitive personal information to access everyday digital tools—which are becoming ever more ubiquitous—would only compound these dangers.

Unfortunately, the privacy dangers of HB1179 do not end there. Parents would be further required to give consent before their children are allowed to download apps. Parental oversight of, and control over, their children's online lives is unquestionably best. However, the process outlined in the bill would compound risks to data security and privacy. Under HB1179, a parent would have to prove his or her relationship to the child, which would inevitably require even more intrusive data gathering to prove both the identity of the parent and his or her status as the child's legal guardian.

Recent experience demonstrates the dangers of exposing large amounts of sensitive information in vulnerable databases—even those purported to be secure. In the digital age, hacks and data leaks are commonplace. Indeed, a Duke University analysis found that more than four in five of companies say they have dealt with a hack.[2] Tech companies—including some of the largest and best protected companies—routinely fall victim.[3]

Even third-party age verifiers, which specialize in the business of age verification, experience cyber incidents. "[T]hese services have suffered cyber events, too," as TPA noted in its recent amicus brief filed at the Supreme Court in *NetChoice v. Fitch*. "Outabox, which provided facial-recognition services to various in-person

[1] https://www.rstreet.org/commentary/child-identity-theft-is-a-huge-problem-the-solutions-are-simple/
[2] https://cfosurvey.fuqua.duke.edu/press-release/more-than-80-percent-of-firms-say-they-have-been-hacked/
[3] https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html

businesses, announced a massive cybersecurity breach in 2024 resulting in the piracy of more than one million consumer records. AU10TIX, an identity-verification service used by recognizable platforms like Uber, TikTok, X, and LinkedIn, is another victim of cybercrime."[4]

Even ostensibly privacy-protective age-verification mandates, such as those recently enacted in France, have exposed consumers to digital dangers.[5] Supreme Court Justice Alito put it best during the oral arguments in *Free Speech Coalition v. Paxton*: "There have been hacks of everything."[6]

Users widely understand the cybersecurity and privacy risks that accompany age verification mandates. In the United Kingdom, which recently enacted a broad age verification mandate in its Online Safety Act (OSA), vast numbers of users flooded app stores to download virtual private networks (VPNs) to avoid the mandate. In just the first few days after the OSA's provisions went into effect, VPN use skyrocketed. Proton VPN reported a 1,400-percent surge in new user registrations.[7] NordVPN reported a "1,000 percent increase in purchases," and many other VPNs reported increased user demand.[8]

Protecting children in the digital world, like protecting children in the physical world, is of the utmost importance. However, particularly when considering regulatory proposals to regulate novel digital technologies, it is critical to understand the unintended second- and third-order consequences that would flow from such proposals becoming law. Increasing experience has shown that age verification cuts directly against the goal of protecting children by exposing their personal information—and that of their families—to cybercriminals. TPA urges the Committee to double-down on a commitment to digital privacy—the only effective basis of personal privacy in a digital age—by rejecting age verification mandates or any other proposals that undermine safety.

Sincerely,

David Williams
President

[4] https://www.protectingtaxpayers.org/press/watchdog-group-files-amicus-brief-defending-mississippian-social-media-users/
[5] https://aiforensics.org/uploads/AIF_report_AgeGO_porn_platforms.pdf
[6] https://www.supremecourt.gov/oral_arguments/argument_transcripts/2024/23-1122_7m58.pdf
[7] https://x.com/ProtonVPN/status/1948773319148245334
[8] https://www.wired.com/story/vpn-use-spike-age-verification-laws-uk/

HB1179_UNF_MTC_Consumer Protection - Application S
Uploaded by: Drew Vetter
Position: UNF

MARYLAND TECH COUNCIL
ADVANCING LIFE SCIENCES AND TECHNOLOGY

House Economic Matters Committee
March 10, 2026
House Bill 1179 – *Consumer Protection – Application Store Accountability Act*
POSITION: OPPOSE

The Maryland Tech Council (MTC), with over 800 members, is the State's largest association of technology companies. Our vision is to propel Maryland to be the country's number one innovation economy for life sciences and technology. MTC brings the State's life sciences and technology communities into a single, united organization that empowers members to achieve their goals through advocacy, networking, and education. On behalf of MTC, we submit this letter of **opposition** to House Bill 1179.

This bill proposes to regulate mobile app stores by imposing age verification requirements and imposing substantial new requirements for age verification, parental consent, consumer protection rules, and penalties. While MTC agrees that protecting minors online is of the utmost importance, we believe that the approach proposed here is overly broad and raises several questions regarding privacy, implementation difficulty, and constitutional and federal preemption concerns. A number of our concerns are laid out below.

First, the bill appears to require age verification for all users of application stores, not just minors. In practice, verifying age at scale would likely require collecting sensitive personal information, such as government identification or biometric data, from every Maryland resident who wishes to download an application. This creates significant privacy and security risks by forcing app stores to collect and store data that many companies do not currently possess. Large, centralized databases of identity information are attractive targets for data breaches and misuse.

Second, the bill runs counter to widely recognized data minimization principles that are embedded in the Maryland Online Data Privacy Act (MODPA). MODPA requires companies to collect only the data necessary to provide a service. Mandating identity or age verification for every user would compel companies to gather far more personal information than is otherwise required simply to download an app. Rather than reducing the amount of personal data in circulation, the bill would substantially increase it.

Third, the bill raises serious First Amendment and constitutional concerns. Courts have repeatedly held that access to lawful online speech is protected by the First Amendment. Requiring age verification as a condition of accessing apps that host speech or information could impose an unconstitutional burden on anonymous access to lawful content. Similar laws attempting to mandate age verification for online services have faced significant legal challenges in federal courts for precisely these reasons.

Fourth, the bill risks creating "consent fatigue." If parents and users are constantly required to approve app downloads, accounts, or disclosures, the volume of requests may lead people to approve them reflexively without meaningful review. Excessive consent prompts can ultimately undermine the very goal of informed parental oversight.

Finally, the bill may conflict with the federal Children's Online Privacy Protection Act, which already establishes a national framework governing parental consent for the collection of data from children under 13. By imposing different or additional requirements at the app store level, the bill could create confusion and compliance conflicts for companies that operate nationwide.

For more information call:
Andrew G. Vetter
J. Steven Wise
Danna L. Kauffman
Christine K. Krone
410-244-7000

ESA Concerns HB 1179_030626.pdf
Uploaded by: Jennifer Gibbons
Position: UNF

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

PDF_[MD] HB 1179_app stores_TechNet.pdf
Uploaded by: margaret durkin
Position: UNF

TECHNET
THE VOICE OF AMERICAN INNOVATION

TechNet Mid-Atlantic | Telephone 717.585.8622
P.O. Box 203, New Cumberland, PA 17070
www.technet.org

March 6, 2026

The Honorable Kris Valderrama
Chair
House Economic Matters Committee
Maryland House of Delegates
231 Taylor House Office Building
6 Bladen Street
Annapolis, MD 21401

RE: HB 1179 (Nkongolo) - Consumer Protection - Application Store Accountability Act – Unfavorable

Dear Chair Valderrama and Members of the Committee,

On behalf of TechNet, I'm writing to share concerns on HB 1179.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes 104 dynamic American businesses ranging from startups to the most iconic companies on the planet and represents five million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

We appreciate the intent of this bill and share the commitment to providing a safe and secure online experience for children. TechNet members strongly believe that children deserve a heightened level of security and privacy online, and the industry is actively working to incorporate protective design features into apps, websites, and platforms. For example, some platforms allow minors to set reminders to take breaks or establish settings that protect them from potential threats or unwanted contact. TechNet members are also including parents and guardians in their child's experiences via parental supervision tools. We believe that empowering parents and guardians and their children to have an informed dialogue about navigating the internet and social media, accompanied with providing them with necessary safety and security tools and features, is a strong approach to children's online wellbeing. TechNet is concerned about HB 1179 for several reasons.

<u>Age Verification</u>

HB 1179 requires app store providers to verify the age of every user before granting access to app downloads, purchases, or usage, regardless of the nature of the app the user seeks to access. This bill does not simply encompass app stores; it

places significant requirements on apps. Because app store is defined so broadly, HB 1179 will encapsulate any application that distributes third-party content (i.e., gaming platforms, video streaming services, voice assistants, and curated content providers). Because most app stores are connected to larger services, this will require age verification at the account-creation stage for more than just app stores – it is effectively age verification for the internet accounts of some of the largest tech brands in the United States, far reaching beyond apps.

Age verification is a complex challenge to address and requires consideration of how to properly balance the interests of privacy and security. Stringent age verification measures could necessitate the collection, processing, and storage of sensitive personal information, such as birth dates and government-issued identification. This could conflict with data privacy principles like privacy-by-design and data minimization, and create new vectors for fraud, as every user in the state would have to prove whether or not they are a minor.

Parental Consent and Controls

Additionally, there are privacy concerns associated with the bill's parental consent requirements. Parental consent entails verifying parental relationships and parental rights, which will likely lead to privacy-invasive processes beyond collecting and verifying the age of an individual. For example, even with a birth certificate, there are custody agreements and other issues that could prevent a caregiver listed on that certificate from exercising parental rights to provide consent. Additionally, the bill is silent on the specific methodologies that would be sufficient to obtain and verify parental consent as well as parental relationships and rights, leading to compliance uncertainty and potential legal vulnerabilities.

Constitutionality

We believe that there are likely constitutional issues with the bill that are similar to those identified by courts with other age verification and parental consent bills. A number of other states that have passed legislation with age verification requirements have had those laws challenged and enjoined due to constitutional concerns. Ohio's *Social Media Parental Notification Act* and Arkansas' SB 396 are recent examples where courts have enjoined the laws from going into effect due to constitutional deficiencies.

In the case of Texas' SB 2420, a federal court found that the law was a content-based restriction on speech that failed strict scrutiny under the First Amendment. The court concluded that SB 2420 "is akin to a law that would require every bookstore to verify the age of every customer at the door, and for minors, require parental consent before the child or teen could enter and again when they try to purchase a book."[1] HB 1179 would likely suffer the same fate.

[1] *Order Granting Motion for Preliminary Injunction*, **CCIA v. Paxton**, No. 1:25-cv-01660 (W.D. Tex. Dec. 23, 2025) (Pitman, J.).

Enforcement

HB 1179 empowers the Attorney General to enforce compliance and allows individuals to file civil lawsuits, via the state's unfair and deceptive trade practices statute, against those who fail to meet the bill's requirements. These provisions create significant legal and financial risks, particularly for smaller developers who may be less equipped to handle litigation. The cumulative impact of new legal obligations, uncertainty in how to comply, and the potential for litigation threatens to stifle innovation. Despite the safe harbor provisions in the bill, TechNet remains concerned about the enforcement provisions.

For these reasons, TechNet respectfully opposes HB 1179. Thank you for considering our concerns, and please feel free to reach out if you have any questions.

Sincerely,

Margaret Durkin

Margaret Durkin
TechNet Executive Director, Pennsylvania & the Mid-Atlantic

HB1179_ACTTheAppAssociation_Stevens.pdf
Uploaded by: Morgan Stevens
Position: UNF

ACT | The App Association

Maryland House of Delegates Economic Matters Committee
230 Taylor House Office Building
Annapolis, MD 21401

March 10, 2026

Chair Valderrama, Vice Chair Charkoudian, and Members of the Committee:

Thank you for the opportunity to speak with you today regarding House Bill 1179.

My name is Morgan Stevens, and I represent ACT | The App Association, a global trade association for small and medium-sized technology companies and independent app developers that drive innovation, job creation, and economic growth across the country, including in the state of Maryland.

ACT and our members share your commitment to protecting children online and empowering parents with meaningful tools to manage their children's digital experiences. We take this responsibility seriously and support policies that genuinely improve online safety without unintentionally undermining privacy, innovation, or legal clarity.

However, HB 1179, as currently drafted, raises serious concerns, particularly for small app developers that do not build products or services specifically designed for or marketed to children. This can include anything from a calculator app to a local pizza place app.

First, the bill establishes broad compliance obligations that are extremely difficult to implement in practice. HB 1179 requires age verification, ongoing parental consent, and reporting app functionality changes. These requirements apply not just to large social media platforms, but to general audience apps—including those used for retail ordering, education, or basic services.

For small developers, building and maintaining these systems is costly, complex, and often unrealistic. Unlike large multinational companies, small businesses do not have compliance teams or legal departments. As a result, some developers may limit features, restrict access for Maryland users, or leave the market entirely, reducing choice and innovation for Maryland families.

Second, HB 1179 would likely increase privacy and security risks. While well-intended, the bill pushes companies to collect and store additional sensitive information to verify age and link parents to children—data they otherwise would not need. More data collection means more risk. Online safety is strengthened when companies collect less personal information, not more.

Finally, HB 1179 raises legal and constitutional concerns. Conditioning minors' access to lawful digital content on age verification and parental consent risks restricting protected

speech for minors and adults alike. These concerns are real. Late last year, a federal court blocked enforcement of a similar Texas app store age-verification law, finding it likely violated the First Amendment.

We share your goal of protecting children online. We believe that goal is best achieved through device-level parental controls, parental education, transparency, and alignment with existing federal frameworks, rather than sweeping mandates that place disproportionate burdens on small businesses.

ACT stands ready to work with Maryland lawmakers on solutions that are effective, privacy-protective, and workable for the innovators serving Maryland families.

Thank you for your time and consideration. I welcome any questions.

Morgan Stevens
Policy Associate
ACT | The App Association

MD HB 1179 - MPA Opposition Letter.pdf
Uploaded by: Renata Colbert
Position: UNF

MOTION PICTURE ASSOCIATION

March 4, 2026

The Honorable Kriselda Valderrama, Chair
House Economic Matters Committee
230 Taylor House Office Building
Annapolis, MD 21401

Re: MD HB 1179 – Application Store Accountability Act

Dear Chair Valderrama and Committee Members:

On behalf of the Motion Picture Association, Inc. ("MPA"),[1] I am writing concerning HB 1179 (the "Bill"), a bill which would create an age verification and parental consent framework for mobile devices. MPA appreciates the concerns that bills like this aim to address, and it supports the goal of helping parents ensure their children have safe, age-appropriate experiences online. Indeed, MPA is an industry leader in providing parents the necessary tools to make informed decisions about what content their children can access—including with its gold-standard content ratings system for motion pictures.[2] However, the Bill as drafted is overbroad and creates cumbersome and impractical burdens on MPA members' streaming services, and critically does nothing to differentiate between applications that have robust age verification and parental controls and those that do not. The Bill would interfere with, rather than promote, existing child safety features that are available on streaming services, and it requires app developers to request minors' data even if the developer has determined not to make its services available to minors.

These concerns are outlined further below, and MPA welcomes the opportunity to work with legislators to address these concerns while continuing to advance the important policy interest of protecting children online.

[1] The MPA serves as the global voice and advocate of the motion picture, television, and streaming industries. It works in every corner of the globe to advance the creative industry, protect its members' content across all screens, defend the creative and artistic freedoms of storytellers, and support innovative distribution models that expand viewing choices for audiences around the world. The MPA's member studios are Netflix Studios, LLC; Paramount Pictures Corporation; Amazon Studios LLC; Sony Pictures Entertainment Inc.; Universal City Studios LLC; Walt Disney Studios Motion Pictures; and Warner Bros. Entertainment, Inc.

[2] *See* Classification and Rating Administration, https://www.filmratings.com/.

I. THE BILL SHOULD DISTINGUISH SERVICES THAT ALREADY MAINTAIN AGE VERIFICATION & PARENTAL CONTROL MECHANISMS

The Bill does not limit its burdens to applications that have no internal age verification measures or which lack parental controls. Instead, *all* applications must request age and parental consent information from a third-party (an app store), even if the service is only available to adult users and/or has parental controls that permit parents to determine what content is available to their children. This one-size-fits-all approach is seeking to mitigate potential harm to children from applications that do not verify ages of their users **and / or** can be accessed with a free login (or no login) with no additional costs to the user or safeguards to prevent minors from accessing inappropriate content. However, this approach does not make sense for services that have direct knowledge of accountholders and have spent years developing and improving protections and parental controls for their users. Notably, the Bill does nothing to require that apps create parental controls or safety features, but it creates liability for those applications that have chosen to create such mechanisms if they do not rely on the third-party signal to enforce such features. Contrary to the Bill's policy objectives, these provisions will only increase the risk of litigation to applications that are trying to do the right thing for their users via age-gating and parental controls.

MPA has an alternative framework which it believes better protects the interests of creating safer online environments for minors, and which recognizes the distinction between services that have adequate safeguards in place and those that may not. To the extent this Bill moves forward, however, MPA seeks amendments that would allow applications like streaming services to continue using their existing, established best practices. For instance, applications that require being an adult to create an account, and which have ratings to permit parents to control their children's access to content, are already satisfying the Bill's policy goals. The Bill should provide a method for developers that voluntarily undertake these measures to continue doing so without participating in a new, bespoke age verification and parental consent framework.

II. THE BILL SHOULD PERMIT SUCH DEVELOPERS TO RELY ON THEIR OWN DATA CONCERNING THEIR CUSTOMERS

The Bill requires that developers not only *request* but affirmatively *rely upon* data gathered by third-party app stores. This risks disrupting user experiences for services, like streaming platforms, that are accessed by multiple individuals within a family across many devices—and it may pose practical barriers when data received by an app store conflicts with data received directly from a customer. Once again, MPA has developed a model framework which takes into account the problem of conflicting data as well as the realities of shared devices and accounts. But absent this alternative approach, the Bill as drafted should be amended to address these concerns.

The Bill requires developers to use the age and parental consent information provided by app stores for a wide range of purposes, including implementing a developer's own age-related restrictions, safety features, and privacy settings, as well as to establish "compliance with applicable laws or regulations." This sweeping obligation could require developers to treat as fact third-party data, that the developer was not involved in collecting or verifying, to fundamentally shape a user's experience—including potentially blocking access to services and features based on the developer's

policies or other state and federal laws. This is particularly impractical as it applies to services that may be accessed on different devices by members of the same family, like a streaming service app that may be downloaded on multiple cellphones, tablets, and televisions. This Bill could require developers to reshape the user experience from one device to another, based on data received *not* from a customer but from a third-party company. In addition, the Bill does not permit a parent to override the signal sent by the third-party app store to the app. The app must rely on the third-party signal or risk being sued for violating the requirements of the Bill.

If this Bill moves forward, it should be amended to permit a developer to rely on their own customer data when offering their services, provided their data is sufficiently reliable, such as data based on a user's credit card information, and the developer chooses to do so.

III. THE BILL SHOULD PERMIT DEVELOPERS TO SET AGE GATES ON APP DOWNLOADS

Additionally, this Bill fails to provide a mechanism for a developer that has determined not to make their service available to children to avoid collecting data about minors. Under the Bill, a minor (with their parents' consent) would be permitted to download *any* application onto a mobile device, and the application developer would then be required to request the user's age and parental consent information—even if the developer did not want to make their application available to minors. The Bill should be amended to add the common-sense requirement that developers can instruct an application store to block downloads for users based on their age as determined by the app store. This will prevent the unnecessary sharing of a user's personal information—including age and parental consent data—for a service that the developer has determined will not be made available to the user.

MPA appreciates the legislature's interest in the issues raised by this Bill, and we are available to discuss alternative frameworks or amendments to the existing framework at your convenience. Please contact Renata Colbert (Renata_Colbert@motionpicturs.org), Nick Manis (nmanis@maniscanning.com), and John Favazza (jfavazza@maniscanning.com) with any questions about the Bill or MPA's proposed amendments.

Sincerely,

Renata Colbert

Renata Colbert
Director, State Government Affairs
Motion Picture Association

* * * *

FINAL MD HB 1179 Testimony - Robert Melvin.pdf
Uploaded by: Robert Melvin
Position: UNF

1411 K St. NW
Suite 900
Washington, D.C. 20005
202-525-5717

Free Markets. Real Solutions.
www.rstreet.org

Testimony from:
Robert Melvin, Northeast Region Director, R Street Institute

In OPPOSITION to House Bill 1179, "Consumer Protection – Application Store Accountability Act"

March 10, 2026

House Economic Matters Committee

Chairwoman Valderrama, and members of the committee,

My name is Robert Melvin, and I am the Northeast Region Director at the R Street Institute (RSI), a nonprofit, nonpartisan public-policy organization. Our mission is to engage in research and outreach to promote free markets and limited, effective government, in a variety of policy areas, including those related to technology and innovation. It's for this reason we are opposed to House Bill 1179.

HB 1179 stipulates that upon setup of a mobile device app stores are required to validate the age of the user and, if the user is determined to be a minor, demonstrate parental consent for every application that is downloaded, updated, or procured by the minor.[1] Although we appreciate the intent of this legislation—protecting kids and teens from harmful content and interactions online—we are troubled by the approach of mandating that all devices and apps acquire age verification.[2] Beyond the significant practical implications this bill presents, HB 1179 has a high probability of being invalidated as an overly expansive and unconstitutional impediment to lawful access to protected expression and content.

To ensure compliance, every mobile device owner, regardless of age, will be required to confirm their age to allow app stores to categorize users into one of four brackets: under 13, 13-15, 16-17, and 18 or older. To determine a user's age group, app stores are permitted to apply "commercially available methods that are reasonably designed to ensure accuracy."[3] Even leading age-verification technologies carry measurable rates of misclassification, and these inherent inaccuracies will predictably compel some adult users to furnish identification of age to avoid being categorized as a minor.[4]

To create parent accounts, adults would likely need to verify their age with government-issued identification to permit minors—up to age 18—to access apps on their devices.[5] While HB 1179 directs that the app stores only keep the data necessary to certify legal compliance with age verification, the prospect of liability under this measure will encourage these companies to preserve more sensitive personal data.[6] This is especially true since, although HB 1179 does not include an explicit private right of action, it is enforceable via the Maryland Consumer Protection Act, which allows individuals to file litigation.

1411 K St. NW
Suite 900
Washington, D.C. 20005
202-525-5717

Free Markets. Real Solutions.
www.rstreet.org

HB 1179 would require app stores to gather additional consumer data, creating a new and attractive target for hackers. Similar security concerns contributed to the courts' decision to enjoin California's Age-Appropriate Design Code, where a district court found the law was "actually likely to exacerbate the problem by inducing covered businesses to require consumers, including children, to divulge additional personal information."[7]

Courts have struck down broad age-gating requirements on general-purpose online platforms as overbroad under the First Amendment, distinguishing them from narrow limits on unlawful or obscene content.[8] Mandates that require parental consent for minors to access lawful, non-obscene content have likewise been struck down. As Justice Scalia observed for the majority, the Court expressed skepticism about "punishing third parties for conveying protected speech to children just in case their parents disapprove of that speech" as a legitimate means of advancing parental authority.[9]

Several states enacted variations of HB 1179 last year, and the first to take effect, Texas SB 2420, was immediately enjoined by a district court.[10] Judge Robert Pitman compared the law's app store age verification requirements to mandating that bookstores verify every customer's age at the door and obtain parental consent for minors before entry and again at purchase, calling the law "unconstitutional in the vast majority of its applications." Considering that HB 1179 is strikingly similar to that law, there is a high probability it would face the same judicial outcome if adopted.

HB 1179 substitutes government intervention for solutions that already exist in the marketplace. Technology firms have committed significant investments to improve parental control tools across devices, browsers and platforms so they are more user-friendly and effective.[11] Moreover, a well-developed ecosystem of third-party software provides parents with advanced tools to monitor and limit their children's mobile device screen time and online activity, and there are online resources that walk parents through the use of child safety settings.[12] The existence and accessibility of these alternatives further demonstrates why broad age verification mandates do not satisfy the First Amendment's requirement to use the least restrictive means to regulate access to objectionable content.[13]

A more constructive alternative to government age verification edicts would be for the state to focus on equipping parents with the knowledge of tools already available to help keep their children safe online, and simultaneously teaching young people how to navigate social media and the internet responsibly. One notable example is Tennessee, which in 2025 enacted a law requiring digital literacy to be incorporated into the state's public school curriculum.[14] The Federal Trade Commission's "Protecting Kids Online" campaign provides another example of how government can support parents in navigating the many parental control tools already available to them.[15] Strategies like these are likely to be more

1411 K St. NW
Suite 900
Washington, D.C. 20005
202-525-5717

Free Markets. Real Solutions.
www.rstreet.org

effective and far more consistent with protecting free expression online than imposing a sweeping age verification mandate.

Finally, this legislation would be easy to bypass. Once granted access to a device the first time, any user could simply use a search engine or browser to access the internet with few limitations. In practice, the bill amounts to little more than security theater, creating the illusion of protection while doing nothing to meaningfully restrict access. A proposal that can be so easily circumvented should give us pause.

For these reasons, HB 1179 presents significant constitutional concerns, creates new privacy and security risks, and attempts to replace existing parental tools and market solutions with an approach that is both easily circumvented and unlikely to survive judicial review. While the goal of protecting children online is an important one that we share, this bill is not the right path forward. Accordingly, we respectfully urge the committee to give HB 1179 an unfavorable report.

Thank you,

Robert Melvin
Northeast Region State Government Affairs Director
R Street Institute
rmelvin@rstreet.org

---

[1] HB 1179, Maryland General Assembly, 2026 Legislative Session. https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/hb1179?ys=2026RS.

[2] See Shoshana Weissmann and Josh Withrow. "No, conscripting the app stores doesn't solve the problems with age verification," R Street Institute, Jan. 29, 2025. https://www.rstreet.org/commentary/no-conscripting-the-app-stores-doesnt-solve-the-problems-with-age-verification/.

[3] Maryland General Assembly, 2026 Legislative Session, House Bill 1179, Last Accessed March 4, 2026. https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/hb1179?ys=2026RS.

[4] On error rates for the best age estimation technologies, see: Kayee Hanaoka, et al., "Face Analysis Technology Evaluation: Age Estimation and Verification," *NIST Internal Report 8525*, May 2024. https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8525.pdf.

[5] "The State of Play: Is Verifiable Parental Consent Fit for Purpose?" *Future of Privacy Forum,* June 2023. https://fpf.org/verifiable-parental-consent-the-state-of-play/

[6] Shoshana Weissmann, "Age verification legislation discourages data minimization even when legislators don't intend that," R Street Institute, May 24, 2023. https://www.rstreet.org/commentary/age-verification-legislation-discourages-data-minimization-even-when-legislators-dont-intend-that/

1411 K St. NW
Suite 900
Washington, D.C. 20005
202-525-5717

---

[7] Adrian Moore and Eric Goldman, "California's Online Age-Verification Law is Unconstitutional," *Reason*, Nov. 28, 2023. https://reason.org/commentary/californias-online-age-verification-law-is-unconstitutional/.

[8] See *Reno v. ACLU*, 521 U.S. 844 (1997), U.S. Supreme Court, June 26, 1997. https://supreme.justia.com/cases/federal/us/521/844, and *Ashcroft v. ACLU*, 542 U.S. 656 (2004), U.S. Supreme Court, June 29, 2004. https://supreme.justia.com/cases/federal/us/542/656/.

[9] *Brown et al. v. Entertainment Merchants Assn. et al.,* 564 U.S. 786 (2011). U.S. Supreme Court, June 27, 2011. https://supreme.justia.com/cases/federal/us/564/786.

[10] CCIA v. Paxton, case n. 1:25-CV-1660-RP (United States District Court Western District of Texas, Austin Division, filed December 23, 2025), https://storage.courtlistener.com/recap/gov.uscourts.txwd.1172869998/gov.uscourts.txwd.1172869998.65.0.pdf.

[11] See, "Helping Protect Kids Online," Apple.com, Feb. 2025. https://developer.apple.com/support/downloads/Helping-Protect-Kids-Online-2025.pdf, "Leading Technology Companies and Foundations Back New Initiative to Provide Free, Open-Source Tools for a Safer Internet in the AI Era," *PR Newswire*, Feb. 10, 2025. https://www.prnewswire.com/news-releases/leading-technology-companies-and-foundations-back-new-initiative-to-provide-free-open-source-tools-for-a-safer-internet-in-the-ai-era-302371243.html.

[12] For example, a quick step-by-step walkthrough for how to enable parental controls on any commonly-owned mobile device: "Parental Controls," Internet Matters, https://www.internetmatters.org/parental-controls/.

[13] Ben Sperry, "The Law & Economics of Online Age Verification and Parental Consent: App Store Edition," *Truth on the Market*, Sept. 26, 2024. https://truthonthemarket.com/2024/09/26/the-law-economics-of-online-age-verification-and-parental-consent-app-store-edition/.

[14] HB 0285, Tennessee General Assembly, 2025 Legislative Session. https://wapp.capitol.tn.gov/apps/BillInfo/default.aspx?BillNumber=HB0825&GA=114.

[15] "How to Use Parental Controls to Keep Your Kid Safer Online", Federal Trade Commission, April 2025. https://consumer.ftc.gov/articles/how-use-parental-controls-keep-your-kid-safer-online.

HB 1179 CPD Letter of Information.pdf
Uploaded by: Hanna Abrams
Position: INFO

CAROLYN A. QUATTROCKI
Chief Deputy Attorney General

LEONARD J. HOWIE III
Deputy Attorney General

CARRIE J. WILLIAMS
Deputy Attorney General

SHARON S. MERRIWEATHER
Deputy Attorney General

ZENITA WICKHAM HURLEY
Deputy Attorney General

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

ANTHONY G. BROWN
Attorney General

WILLIAM D. GRUHN
Division Chief

PHILIP ZIPERMAN
Deputy Division Chief

PETER V. BERNS
General Counsel

CHRISTIAN E. BARRERA
Chief of Staff

HANNA ABRAMS
Assistant Attorney General

March 10, 2026

TO: The Honorable Kriselda Valderrama, Chair
Economic Matters Committee

FROM: Hanna Abrams, Assistant Attorney General

RE: House Bill 1179 – Consumer Protection – Application Store Accountability Act (LETTER OF INFORMATION)

The Consumer Protection Division of the Office of the Attorney General (the "Division") submits this letter of information regarding House Bill 1179 ("HB 1179"). House Bill 1179 creates age verification obligations for app stores and app developers.

While the Division is not taking a position on the merits of HB 1179, the Division notes that the bill requires app developers and app stores to verify the age category of account holders. At the same time, the Maryland Age-Appropriate Design Code Act prohibits the "process[ing of] any personal data for the purpose of estimating the age of a child that is actively and knowingly engaged with an online product that is not reasonably necessary to provide the online product."[1] Although the scope of each bill is slightly different, there is potential for overlap. The inconsistency between their respective requirements may create ambiguity and lead to confusion about implementation.

House Bill 1179 would also require the Division to issue regulations. The Division respectfully requests that the "shall" on page 11, line 3 be replaced with "may."

Finally, HB 1179 permits the Attorney General to recover civil penalties of $7,500 for each violation on top of the penalty provisions of the Consumer Protection Act (page 11, lines 12-15). While the Division believes this provision is intended to authorize it to penalize violators with an additional $7,500 per violation beyond penalties recovered for violations of the Consumer Protection Act, the intent would be clearer if the provision instead used the following language:

[1] Md. Code Ann., Com Law § 14-4806(a)(8).

In addition to the remedies provided under Title 13 of this article, the Division may also recover civil penalties not to exceed $7,500 for each violation under this subtitle.

The Division respectfully requests that the Economic Matters Committee consider the concerns discussed above when it considers HB 1179.

cc: Delegate LaToya Nkongolo
Delegate Steven J. Arentz
Delegate Kevin B. Hornberger
Delegate April Miller
Delegate Chris Tomlinson
Members, Economic Matters Committee