



27 February 2025

Dear Honorable Members of West Virginia's House Environment, Infrastructure, and Technology Subcommittee:

We are writing in support of the App Store Accountability Act (HB2609). Michael Toscano is the director of the Institute for Family Studies. In November 2023, Michael co-published a paper with leading tech policy scholar Clare Morell, titled, "[Making Smartphones and App Stores Safe for Kids,](#)" which legislation like WV XXX is based on. He has been a supporter of the App Store Accountability Act since its inception. Jared Hayden is a policy analyst at the Institute for Family Studies and has testified in support of legislation requiring age verification and parental consent at the app store level in other states.

We support this bill because it applies common sense to the conduct of app stores and restores to parents basic rights that have been taken from them by how app stores operate.

Despite the fact that the [majority](#) of parents limit their teen's digital usage, [most](#) remain worried that they will be exposed to harms online. Such worries are not ill-founded. Compared to every other industry, tech companies face effectively no liability for failing to provide commonsense safeguards such as age verification or parental consent for their products.

In any other market setting—from banks to supermarkets—it is unimaginable that children would be allowed to enter contracts or purchase risky products without verifying their age or getting parental consent. Yet, despite having the technological ability to effortlessly implement such safeguards, these companies refuse to do so, and parents are left powerless to protect their families when parental controls inevitably fail.

In order to help parents and protect kids, we must end app store exceptionalism—which HB2609 does. Only in app stores do we allow minors to enter into terms of service agreements with trillion-dollar companies that determine how their personal data can be used. Only in app stores do we give such companies full access to extremely sensitive information like personal photographs and videos of children, their exact location, and their contact lists. In a brick-and-mortar, such requests would be greeted with suspicion and alarm. In a brick-and-mortar we would protect our kids from providing such material, knowing that anyone that wanted it would be a threat to their best interests. This bill ends app store exceptionalism by requiring parental consent for all app downloads, app-purchases, and in-app purchases.

---

**The Future Is Family**

P.O. Box 1502 Charlottesville Virginia, 22902  
434-326-7583 | [michael@ifstudies.org](mailto:michael@ifstudies.org)  
[www.ifstudies.org](http://www.ifstudies.org)



There is no reason why app stores should be allowed to contract with someone who is above thirteen years of age when in the real world you have to be 18 to form a valid contract. States are within their rights to empower parents to exercise authority over the contracts that their children form in the app store. Opponents of this bill say that the Children's Online Privacy Protection Act (aka COPPA) sets an age ceiling of 13-years old for the requirement of parental consent, giving apps the power to engage with older children however they wish. But this is wrong. COPPA regulates how companies gather data; the App Store Accountability Act, by contrast, regulates how companies contract with minors. COPPA does not preempt this bill. This bill fixes the bizarre mismatch between how states regulate contracts in the digital world and real life, setting them both at 18.

If passed, this bill would establish (long overdue) commonsense safeguards for kids in the digital age. Having worked for the past two years with advocates, tech experts, and Constitutional lawyers on bills like this, we are confident that HB2609 is a technologically feasible, privacy protecting, and constitutional bill that will make app stores safer for kids and put parents back in the driver's seat.

Sincerely,

Michael Toscano  
Director, Family First Tech Initiative, Institute for Family Studies

Jared Hayden  
Policy Analyst, Family First Tech Initiative, Institute for Family Studies

---

**The Future Is Family**

P.O. Box 1502 Charlottesville Virginia, 22902  
434-326-7583 | michael@ifstudies.org  
www.ifstudies.org

## **International Centre for Missing and Exploited Children (ICMEC) - West Virginia HB 2609**

Date: February 27, 2025

Thank you for the opportunity to provide this written support for HB 2609. My name is Bob Cunningham, and I am the Director of Policy Engagement for the International Centre for Missing & Exploited Children (ICMEC, see [www.icmec.org](http://www.icmec.org)), a nonpartisan U.S. based nonprofit organization with a 25 year history of working globally to protect children from sexual abuse and exploitation in all forms.

Age verification is an important and complex problem foundational to protecting children from harm, and ICMEC strongly supports the device-based verification solution required under West Virginia HB 2609. ICMEC believes that such a solution is necessary in order to effectively protect children online. The reality is that every member of the digital ecosystem – from the device manufacturer and operating system, to the application store, app, and website – should be held responsible for child protection.

In line with our support of a device-based age verification mechanism, ICMEC also strongly advocates to expand the digital age signal prescribed by HB 2609 so that it can be sent from an operating system to websites and online services. By expanding the digital age signal to websites that have a legitimate need to receive the signal, we can ensure that children are fully protected wherever they go online. By including websites in the digital age signal, this will cover circumstances where children access the browser version of an application and eliminates opportunities for circumvention, including through basic methods such as a VPN.

ICMEC views device-based age verification as the most common sense and feasible solution. It is an industry-wide solution that holds all online services in the online journey of a child accountable for their safety. It is also a secure approach in that, rather than providing personal information to dozens of websites and applications, all of which may have varying levels of security and privacy practices, device-based age verification centralizes the point of verification at the lowest common denominator: on the device itself.

Overall, device-based age verification is a technically feasible, constitutionally sound method of age verification that protects the privacy of both adult and child users. It does not disclose the identity of a child or adult; once a user verifies on their device, they are wrapped in a shroud of privacy that securely provides websites and applications only with a user's encrypted age range. This bill provides a critical tool to protect vulnerable children in West Virginia, children whose parents may not be involved or aware of their child's digital experience, and it minimises the opportunity for children to find ways around website or app based verification through means such as using a VPN. It ensures a uniform and effective age verification mechanism that could eventually be deployed globally, which is significant since online harms are borderless, and online protection is a worldwide imperative.

I urge you to pass this important bill and to incorporate websites in HB 2609 to further expand the protections offered to children. Thank you for your time and consideration.

Robert B. Cunningham  
Director of Policy Engagement  
International Centre for Missing & Exploited Children  
[bcunningham@icmec.com](mailto:bcunningham@icmec.com)



# NATIONAL CENTER ON SEXUAL EXPLOITATION

EndSexualExploitation.org

February 24, 2025

The Honorable Members of the House Environment, Infrastructure, and Technology Committee  
State Capitol – Building 1  
1900 Kanawha Blvd E  
Charleston, WV 25305

## **RE: Support for H.B. 2609 Limiting Teen Access to Inappropriate Material**

Dear Honorable Members of the Committee:

On behalf of the National Center on Sexual Exploitation, I am writing to urge your support of H.B.2609: Limiting teen access to inappropriate material. This is a critically needed solution, however a few amendments are needed to the bill and we will gladly work with the sponsor to ensure those make it in. We strongly urge you to allow this bill to move forward.

As an organization dedicated to protecting children and families from sexual exploitation, we have been advocating for app store accountability since 2017. Seven other states are considering similar legislation this year and a federal version will move forward next month. You will be in great company as states across the U.S. push for improved solutions to protect children and empower parents.

While a multi-layered approach to online child safety is essential, this legislation fills a critical gap that has been missing for far too long. **App stores serve as the gatekeepers of the digital world, yet they routinely fail to protect children.** The measures outlined in this bill would significantly address several urgent issues and create a safer online environment for millions of families.

### **1. Parental Consent**

Children as young as eight years old routinely download apps and agree to Terms of Service contracts without their parents' knowledge or understanding of the risks. Some of these agreements allow sensitive personal information—including exact locations, full names, dates of birth, and school names—to be collected and shared broadly. This has led to devastating consequences.

For example, we know of a young girl whose location data was shared through an app, enabling a predator to find her in real life. Stories like these are far too common, and this bill ensures that parents, not corporations, have the final say in their children's digital activities.

### **2. Accurate and Transparent Age Ratings**

The current app store age rating system is dangerously misleading. One of the most egregious examples is Roblox, a popular app advertised as “made for kids under 13” and historically rated for ages 4+ and 9+. Parents trusted these ratings and millions enabled parental controls to prohibit communication with strangers, believing their children were safe.

However, even with these controls, children are routinely exposed to sexually explicit material and predators who exploit them in virtual games. Thousands of children have fallen victim to predatory grooming, sexual abuse, sex trafficking, and even kidnapping as a direct result of predators gaining access to children on Roblox. Accurate age ratings and content descriptors are not optional—they are a matter of safety and trust.

### **3. Age Verification**

App stores already collect and manage age data through systems like Apple’s Family Sharing and Google’s Family Link. They have the technical capability to verify user ages securely and share anonymized age information with developers. These tools are already being used in other contexts (such as for gambling apps in some states and for the Apple/Google payment systems), and this bill simply requires app stores to leverage them to protect children.

By verifying user ages, app stores can ensure that children are accessing age-appropriate content and that developers can comply with federal laws like COPPA. This step alone would prevent countless instances of children being exposed to harmful content or manipulated by apps designed for older users.

**The App Store Accountability Act is not just another layer of protection—it is a fundamental solution that addresses the root causes of so many harms children face online.** By ensuring parental consent, accurate age ratings, and verified ages, this bill empowers parents, safeguards children, and holds app stores accountable for their role as digital gatekeepers.

We urge you to support and advance this legislation. The stakes could not be higher, and the opportunity to make meaningful progress in protecting children is now. If we can provide further information or assistance, please do not hesitate to reach out at [hawkinsd@ncose.com](mailto:hawkinsd@ncose.com).

Thank you for your leadership and commitment to safeguarding our children and families.

Sincerely,



Dawn Hawkins  
Senior Advisor, National Center on Sexual Exploitation

February 27, 2025

Committee on Environment, Infrastructure, and Technology  
West Virginia House of Representatives  
1900 Kanawha Blvd. E.  
Charleston, West Virginia 25305

Dear Chair Linville, Vice Chair Hillenbrand, and members of the committee:

On behalf of the millions of taxpayers and consumers we represent, the Taxpayers Protection Alliance (TPA) urges you to oppose HB 2609, the Digital Age Verification Act. This legislation presents deep constitutional issues both from its mandate for device manufacturers to estimate or verify their users' age, and the requirement that any device activated in the state of West Virginia to have a preconfigured filter that would block access to content deemed mature during the activation of the device by a minor.

The issues with this bill, as currently drafted, are twofold. First, the constitutionality of age verification legislation remains – at best – highly questionable. In *NetChoice v. Griffin* (2023), a district court blocked a similar Arkansas bill requiring social media platforms to obtain age-verification and parental consent due to the high potential it unconstitutionally violated the First Amendment. According to the American Civil Liberties Union, “Individuals of all ages rely on social media for political speech, artistic expression, advocacy, access to the news, and more. Imposing unconstitutional age-verification requirements burdens users who may want to engage in anonymous speech, who do not have government ID, and who are otherwise concerned about their privacy and security. The legislation’s parental consent requirement would also impermissibly burden the First Amendment rights of young people, who are often at the forefront of movements, trends, and technologies.”<sup>1</sup>

Enacting this age verification mandate at the device or app store level would not curtail the constitutionality issues, as users’ first amendment right to anonymously navigate or express themselves online would still be trampled on. These mandates also force app store developers to collect and harvest significant amounts of personal data from its users. Currently, these developers rely exclusively on users’ self-reported ages to fulfill compliance requirements from existing regulations, such as the Children's Online Privacy Protection Rule. However, the bill’s requirement that app store developers must use age verification and estimation technologies would force companies to not only collect information at the moment of account creation, but to perpetually monitor users’ online activity to validate that the initial age verification was accurate. This requirement would contravene the national push for higher privacy standards in consumer technology.

Additionally, while well-intentioned, “device filter” bills are riddled with constitutional issues. Seeking to protect children online is a noble goal, but device filter mandates are unconstitutional because they automatically block protected speech for users of all ages and are technically impractical to implement for industry actors.

By requiring content filters to be automatically enabled on connected devices, these filters would act as blockers of constitutionally protected expression. The First Amendment is silent on how offensive or objectionable the content may be. Most of the Communications Decency Act of 1996 was struck down in *Reno v. ACLU* because of how restrictive the Act was compared to alternatives to achieve its intended purpose. As Justice John Paul Stevens wrote in his opinion, “It is true that we have repeatedly recognized the governmental interest in protecting children from harmful materials. But that interest does not justify an unnecessarily broad suppression of speech addressed to adults.”<sup>2</sup> Device filter bills do exactly that.

Similar age restrictions to protected speech have also been ruled unconstitutional in *Brown v. Entertainment Merchants Association*. This case determined that banning violent video games for minors was unconstitutional.<sup>3</sup> Banning minors from accessing content on their handheld devices will likely come under similar scrutiny and be challenged in the Courts.

There are already industry solutions when it comes to parental controls and filtering obscene online content. As TPA has stated previously in our analysis of device filters mandates as a concept, “There is no argument against devices and services having parental controls. Virtually every device manufacturer, online platform, and internet service provider (ISP) have them

<sup>1</sup> <https://www.aclu.org/press-releases/judge-blocks-arkansas-law-that-would-have-placed-unconstitutional-age-verification-and-parental-consent-requirements-on-social-media-users>

<sup>2</sup> *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

<sup>3</sup> *Brown v. Entertainment Merchants Association*, 564 U.S. 844 (2011).

**TAXPAYERS  
PROTECTION  
ALLIANCE**

as options and provide them free of state coercion... Turning these features on by default through the force of law, however, is inherently a restriction on otherwise legally protected speech.”<sup>4</sup>

This bill is undoubtedly well-meaning, but it presents serious constitutional issues and would get the state involved in frivolous lawsuits that would cost taxpayers’ money. It would be in the best interests of taxpayers and consumers in West Virginia for this committee to reject HB 2609 and any bills like it.

Sincerely,



David Williams  
President

---

<sup>4</sup> <https://www.protectingtaxpayers.org/internet/device-filter-bills-reveal-inconsistency-on-outsourced-censorship/>

## West Virginia HB 2609

## TESTIMONY IN OPPOSITION

February 25, 2025

**West Virginia House of Delegates  
Committee on Energy and Public Works  
Subcommittee on Environment, Infrastructure, and Technology**

Dear Chair Linville, Vice-Chair Hillenbrand, and Members of the Subcommittee on Environment, Infrastructure, and Technology:

NetChoice is a principles-based trade association that works to make the Internet safe for free enterprise and free expression. In line with that mission, we are also dedicated to advancing policy that will effectively protect children and families online. However, for several reasons, HB 2609 falls short of this goal. We respectfully ask that you **oppose** HB 2609 because the bill:

1. Violates the First Amendment
2. Creates unnecessary risks and harms for users of all ages
3. Would be ineffective at meaningfully inhibiting access to online harms

### HB 2609 violates the First Amendment

Congress passed the Communications Decency Act in 1996. The law was an attempt to restrict the access of minors to obscene content on the internet. The legislation criminalized the “knowing” dissemination of “obscene or indecent” material or knowingly sending messages “that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs” to those under the age of 18.<sup>1</sup> It created safe harbors for those who made good faith attempts to restrict minors’ access to such content.<sup>2</sup>

The law was quickly enjoined and then struck down as unconstitutional. The federal government lost on appeal to the Supreme Court in the 9-0, landmark case, *Reno v. ACLU*. The Supreme Court held that the broad nature of the restrictions, their punitive nature, and their attachment to a medium which

<sup>1</sup> Cornell Law school, Legal Information Institute, [Reno v. ACLU | US Law | LII / Legal Information Institute \(cornell.edu\)](#)

<sup>2</sup> *Ibid*

enjoys full First Amendment protections, among other issues, were enough to rule that the Communications Decency Act was violative of the First Amendment.

Unlike the unconstitutional Communications Decency Act, however, HB 2609 makes no effort to even target obscene or indecent content. The bill would impair access to perfectly benign apps, even those explicitly designed to be child-friendly. Adult users, too, would be burdened with age verification before downloading and accessing everything from browsers to video streaming to delivery apps.

The sponsors of HB 2609, just like Congress in 1996, are concerned with the welfare of children online. That is a laudable goal, and one that NetChoice shares. The reality however, is that the Supreme Court looks more seriously at unintended negative consequences to constitutional rights rather than well-intentioned goals. There is no question, seeing as the issues at the core of both cases are nearly identical, with HB 2609 sweeping up far more kinds of content, that this bill would quickly meet the same fate as the Communications Decency Act.

Several state laws aimed at requiring age verification for online access are being challenged in federal courts on constitutional grounds. Federal judges have preliminarily blocked these laws in multiple states - including Arkansas<sup>3</sup>, California<sup>4</sup>, Mississippi<sup>5</sup>, Ohio<sup>6</sup>, Texas<sup>7</sup>, and Utah<sup>8</sup> - pending full legal review of the challenges. A similar legal challenge to HB 2609 would bring confusion and significant cost to West Virginia taxpayers. That would best be avoided.

## **HB 2609 creates unnecessary risks and harms for users of all ages**

Aside from the constitutional issues surrounding mandatory age verification, there are several practical issues that present unacceptable tradeoffs for users of all ages. First and foremost is user privacy. HB 2609 would force all device manufacturers to collect and store sensitive information about users, particularly government-issued IDs, in order to use their devices to their full potential. Adding HB 2609 to West Virginia's statutes would signal to bad actors that stealing or otherwise breaching any personal device would almost assuredly yield access to this information.

---

<sup>3</sup> NetChoice, LLC v. Griffin (W.D. Ark. 2023)

<sup>4</sup> NetChoice v. Bonta (N.D. Cal. 2024)

<sup>5</sup> NetChoice, LLC v. Fitch (S.D. Miss. 2024)

<sup>6</sup> NetChoice, LLC v. Yost (S.D. Ohio 2024)

<sup>7</sup> Computer & Communications Industry Association v. Paxton (W.D. Tex. 2024)

<sup>8</sup> NetChoice, LLC v. Reyes (D. Utah 2024)

To ensure compliance with the developer-side requirements of the bill, app developers would need to log user data, such as time and location, and the age signal received each and every time a user opens the app. While HB 2609 appears to only require signaling age information upon device activation and installation of new apps, the reality is that because the age categories of users and parental permissions will naturally change over time, apps cannot rely solely on the initial age information provided by the app store, necessitating constant collection and cataloguing of additional user data.

Age verification technology remains unproven and insufficiently secure. There are countless examples of high-profile hacks of concentrated collections of sensitive data, from the federal Office of Personnel Management<sup>9</sup> to health insurance exchanges created by the Affordable Care Act.<sup>10</sup> Concentrating sensitive data creates a bullseye for bad actors. Age verification systems create such a target, demonstrated by the recent hack of an age verification system used in Australia to verify and store the information of adults accessing physical locations with age restrictions, such as bars.<sup>11</sup> The requirements of HB 2609 would necessitate creating caches of sensitive data, including personal identification, of all West Virginia users *regardless of their age*.

An additional harm certainly worth mentioning is the fact HB 2609 would unintentionally discriminate against the most vulnerable children in society. The bill requires parental consent for children to download and access *any* application, not just those inappropriate for children. This would pile on an exceptional disadvantage for at-risk children in broken homes, the foster care system, and other situations lacking the ability to secure parental consent. These children would be denied access to educational tools and services in app stores, driving an even greater wedge between them and their peers.

## **HB 2609 would not meaningfully inhibit access to online harms**

While HB 2609 would be extremely effective at burdening access for West Virginians of all ages to any applications regardless of content and use, it would do little to substantially inhibit the ability of minors to reach harmful corners of cyberspace. In fact, the bill would likely increase the chance of users, particularly children, encountering online harms.

---

<sup>9</sup> Sciutto, Jim, "OPM government data breach impacted 21.5 million," CNN, July 10, 2015, <https://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/index.html>

<sup>10</sup> Mandler, C., "Following a 'significant' breach, DC Health Link user data is being sold on the dark web," CBS News, March 8, 2023, <https://www.cbsnews.com/news/data-breach-washington-dc-health-link-user-data-sold-dark-web-congress/>

<sup>11</sup> Kidd, Jessica, "Cybercrime detectives arrest man following alleged data breach involving more than 1 million NSW clubs customer records," ABC News, May 1, 2024, <https://www.abc.net.au/news/2024-05-02/clubs-nsw-cybersecurity-potential-data-breach-venues/103793584>

First, the bill says nothing about access to harmful content through browser apps shipped with devices. Instead of accessing the application-side of various platforms, teens can easily view and interact through website versions.

Further, despite listing laptops and desktops in the definition of covered devices, HB 2609 neglects to address the fact that laptops and desktop computers allow download and installation of software from the open web. Even Apple, known for its walled-garden approach to iPhones and iPads, allows for direct downloads of software on its Mac laptops and computers. All HB 2609 would do is drive users away from app stores on these devices, which provide an added layer of vetting and security, and towards less-safe direct downloads from the open web. This increases the chance that users, particularly teens looking to get around age verification, will accidentally load their computers with malware.

Finally, an awful but predictable side effect of HB 2609 is that the bill would give parents a false sense of security. Filtering technology is only so precise, and HB 2609 leaves countless content access methods uncovered. HB 2609 sends a false “all-clear” message to parents who would otherwise remain vigilant in supervising their children's online activity.

---

The problem HB 2609 seeks to tackle is not without solutions that are both constitutional and practical. Florida<sup>12</sup> and Virginia<sup>13</sup> have passed laws to facilitate specific online and social media education in the classroom. This helps arm young people and their parents with the information they need to keep their data more secure, focused on age appropriate content, and away from bad actors who would do them harm. West Virginia could take steps to publicize the resources that are available to filter content or monitor and control screen time. Solutions for families and kids do not need to come in the form of government mandates.

For these reasons, we respectfully ask you to **oppose HB 2609**. As ever, we offer ourselves as a resource to discuss any of these issues with you in further detail, and we appreciate the opportunity to provide the committee with our thoughts on this important matter.

Patrick Hedger  
Director of Policy, NetChoice<sup>14</sup>

*NetChoice is a trade association that works to protect free expression and promote free enterprise online.*

---

<sup>12</sup> Laws of Florida Chapter 2023-36, <https://laws.flrules.org/2023/36>

<sup>13</sup> Code of Virginia § 22.1-24.1. (Effective until July 1, 2024) Internet Safety Advisory Council, <https://legacylis.virginia.gov/cgi-bin/legp604.exe?231+ful+CHAP0111+pdf>

<sup>14</sup> The views of NetChoice expressed here do not necessarily represent the views of NetChoice members.