My name is Stephanie, and I am writing because I am against H 7953 – Rhode Island Social Media Regulation Act. As it currently exists, the proposed bill calls for people to upload their government-issued IDs to verify their ages, to prevent teens and children from holding social media accounts. To call this an age verification bill is disingenuous, as it is really an identity verification bill, and many Rhode Island residents are justifiably hesitant with providing *even more* personally identifying information online, in an era where online privacy is being eroded, and effective recourse for personal information being stolen is limited and slow-moving. Teens should absolutely be protected, but age verification laws impact all users, adults and minors alike.

I agree that the Internet can be dangerous, and social media certainly has a number of spaces that are not suitable for minors, but laws that require people to verify their age or identity is an overreach. Common methods for verification include by uploading government-issued IDs, scanning their faces, or providing credit card information. Age verification laws put people at risk, impact their freedom of speech, and unfairly disenfranchise those who do not have an ID. If AI facial scanning becomes an option, please know that AI can be discriminatory towards people of color and those with disabilities, as AI often fails to accurately estimate the ages of people with darker skin or facial deformities (Alajaji). Additionally, "those that lack any acceptable form of identity to prove their age may be excluded from accessing content protected by the First Amendment…simply because they do not have access to a government-issued ID or credit card," (Forland).

The risk of providing personal information online is also not solely whether or not a company retains your ID, but also what other entities that information is shared with, and where it eventually ends up. H 7953 states that social media platforms would only collect information to verify people's ages, and then they would have to delete that information, but they never do, or they fail to do so properly. Having direct confirmation of people's identities is the Holy Grail to these companies. Amassing large amounts of personally identifying information (PII) means that websites and third party age verification vendors become attractive targets for cybercriminals. Data breaches impact millions of people every year, with almost half of all global data breaches impacting PII (Statista), but there is a difference between having an email address or password leaked, versus having your driver's license or full credit card information stolen.

Even when websites and apps have stated that they do not retain personally identifying information, they hold onto it. An app called "Tea" was breached last year, and over 13,000 selfies and photos of IDs used for verification collected prior to 2024 were leaked (Wiseman). Discord, one of the largest, most popular messaging platforms, used a third-party vendor to verify people's ages using their government IDs. The service site was breached, and the IDs of over 70,000 people were compromised (Goodin). Even companies that specialize in verifying identities are at risk. In 2025, IDMerit was discovered to have an exposed database of 1 billion records, containing "full names, home addresses, dates of birth, national ID numbers, phone numbers, email addresses and gender information," (Toledo). The technology used to verify people's ages is also flawed, as it is still being developed. Roblox has begun requiring users to prove their ages, either by uploading ID or taking selfie videos, but the AI used to verify users is flawed, often incorrectly sorting people into younger or older age groups, which exposed children to adult users (Gilbert).

Similar legislation to H 7953 has faced issues with negatively impacting Freedom of Speech, as, while laws restricting access to porn sites often get a pass with age restriction laws due to "the historical tradition of restricting minors' access to sexually explicit material," (Ford), social media is different, as it is not inherently illicit. Many people use social media to not just stay connected with friends and family, but to access news, conduct research, discover local events, promote their businesses, and provide commentary and information to their communities. It has been found previously in court cases that "…age verification mandates would…limit access of adults without acceptable identification… [and] [a]ge verification requirements also leave no space for users who do not wish to identify themselves online, threatening individuals' right to anonymous speech, which has long been upheld by the Supreme Court," (Forland).

While online age verification laws are still in their infancy, a study conducted by the Phoenix Center shows that "age verification laws may be least effective at blocking motivated teenagers who are the primary

policy concern. Meanwhile, age verification laws impose costs on adults who either face friction using VPNs or simply abandon attempts to access legal content… Less tech-savvy adults—who have full constitutional rights to access adult content—bear the highest burden," (Ford). There's nothing stopping teenagers from attempting to circumvent age verification rules with something as simple as taking their parent's ID and using it to access their accounts. There are parents who will allow their teens to access social media on shared devices, despite the ban.

Age verification is difficult to implement fairly, and when it is forced upon people, they are reluctant or unwilling to provide PII, with good reason. Requiring ID to access social media accounts (many of which may have been held by adults for over a decade by now), puts people's privacy and personal information at risk, and restricts their First Amendment rights.

Something to consider is legislation recently passed in North Carolina, mandating that schools must provide instruction regarding social media and its effects on health a number of times throughout middle school and high school (House Bill 959). The best way to protect kids is to prepare and educate them, not keep them ignorant.

I understand the desire to protect kids. But there are more adults online than there are children, and they deserve protection too. I hope it's something that elected officials would take into consideration when creating legislation that will impact everyone in the state.

Thank you.

Sources

2025-2026 General Assembly. "2025-2026 General Assembly House Bill 959: Social Media Literacy in Schools." *Ncleg.Gov*, 21 May 2025, dashboard.ncleg.gov/api/Services/BillSummary/2025/H959-SMBE-39(e2)-v-3.

Alajaji, Rindala. "10 (Not so) Hidden Dangers of Age Verification." *Electronic Frontier Foundation*, 12 Dec. 2025, eff.org/deeplinks/10-not-so-hidden-dangers-age-verification.

Ford, George S. "Unintended Consequences of Age Verification Laws: Evidence from Search Behavior." *Phoenix Center for Advanced Legal and Economic Public Policy Studies*, 12 Nov. 2025, phoenix-center.org/perspectives/Perspective25-06.pdf.

Forland, Sarah, et al. "Age Verification: The Complicated Effort to Protect Youth Online." *New America*, 22 Apr. 2024, ietf.org/agews-paper-age-verification-the-complicated-effort-to-protect-youth-online.pdf.

Gilbert, David. "Roblox's AI-Powered Age Verification Is a Complete Mess." *Wired*, 13 Jan. 2026, wired.com/story/robloxs-ai-powered-age-verification-is-a-complete-mess/.

Goodin, Dan. "Discord Says Hackers Stole Government Ids of 70,000 Users." *Ars Technica*, 9 Oct. 2025, arstechnica.com/discord-says-hackers-stole-government-ids-of-70000-users.

Statista Research Department. "Topic: Data Breaches Worldwide." *Statista*, 17 Dec. 2025, statista.com/data-breaches-worldwide.

Toledo, Marie Joy. "IDMERIT Data Leak Exposes 1 Billion Identity Records - Are You at Risk?" *International Business Times*, International Business Times, 12 Mar. 2026, ibtimes.com/idmerit-data-leak-exposes-1-billion-identity-records.

Wiseman, Paul. "The Tea App Was Intended to Help Women Date Safely. Then It Got Hacked." *AP News*, AP News, 27 July 2025, apnews.com/article/tea-app-data-breach-leak-4chan.