

March 3, 2026

The Honorable Brett Guthrie  
Chairman  
House Committee on Energy and Commerce  
2125 Rayburn House Office Building  
Washington, D.C. 20515

The Honorable Frank Pallone, Jr.  
Ranking Member  
House Committee on Energy and Commerce  
2322 Rayburn House Office Building  
Washington, D.C. 20515

**Re: Privacy, Security, and First Amendment Concerns Regarding Proposed Age Verification Mandates**

Dear Chairman Guthrie and Ranking Member Pallone:

We write on behalf of the Age Verification Providers Association, the global trade body representing suppliers of privacy-preserving, standards-based online age assurance technologies.

We have reviewed the February 18, 2026 letter submitted by Americans for Prosperity, the Center for Democracy and Technology, and the Software & Information Industry Association. While we agree that privacy, security and constitutional rights must be safeguarded, the letter reflects an outdated understanding of modern age assurance technologies and creates a false dichotomy between child protection and civil liberties.

Protecting minors online does not require the creation of centralized identity databases, nor does it require platforms to collect government identification documents. Contemporary age assurance systems are specifically designed to avoid those outcomes. Indeed, the essence of age verification is proving your age *without* disclosing your identity.

**Privacy and Data Minimisation**

Modern age assurance systems are built around data minimization principles and operate without transmitting identity information to content providers at all.

- Independent third-party verification allows a user to prove they are over a required age threshold without revealing identity to the service they are accessing

- Age verification providers can transmit only a “yes / no” age-range attribute e.g “18+”
- Tokenized approaches allow for a single age check to be used across multiple apps and websites
- Double-blind architectures, originally designed by the French data protection regulator, the CNIL, prevent the age assurance provider know which sites are being accessed, and the sites from learning the identity of the user.

These approaches are reflected in international standards, including IEEE 2089.1 and ISO/IEC 27566-1, against which age assurance systems can be independently audited and certified to confirm their accuracy, data security and privacy-by-design qualities.

Contrary to the suggestion that age verification mandates necessarily create “massive databases of identity documents”, the best-practice model is precisely the opposite: separation of roles, minimal data disclosure, and zero retention of personal data (if it is even needed in the first place) once the user’s age range has been established.

### **Accuracy and Technological Maturity**

The assertion that age technologies are inherently inaccurate or immature does not reflect the current state of the market.

Age assurance is not a single technology. It is achieved through a wide choice of methods, including:

- Document verification with high-assurance fraud detection
- Confirmation from authoritative records held by financial institutions or other regulated entities.
- Age inferred from the historic use of a cellphone number or email address
- Biometric age estimation (facial patterns, hand movement and emerging methods such as EKG analysis)
- Reusable digital credentials issued once and presented many times with selective disclosure of only age-range

(Where facial age estimation is used, this is based on a mathematical map of facial features which is not unique to the user so cannot be used for identification, and these maps can be analysed on a user’s own device, or in any case are immediately deleted.)

### **First Amendment Considerations**

Age assurance, when properly designed, does not eliminate anonymity. It completely separates identity from age eligibility.

A user can demonstrate that they are over 18 without disclosing their name, address, specific date of birth or government ID to a website. That is fundamentally different from identification. If American

technology can put a man on the moon, it can let him prove his age online without revealing his identity. It is, literally, not rocket science.

Courts have long recognized that states may adopt measures to prevent minors from accessing material that is harmful for them, provided the measures are proportionate and do not unduly burden adults. The constitutional analysis therefore turns on implementation design. Already, we see the deployment of interoperable, tokenized ecosystems, where a single age check can be used across multiple services, often with no further action required by the user for subsequent sites/apps.

### **Avoiding False Trade-Offs**

The debate should not be framed as mandatory ID uploads versus complete anonymity. There is a separate path: proportionate, standards-based, privacy-enhancing age assurance.

These systems are already operating at national scale in regulated environments. Several jurisdictions, including the United Kingdom, parts of the European Union, Australia and multiple U.S. states, are implementing such systems and our members have completed over a billion age checks. The policy challenge is to ensure interoperability, accountability and competition while avoiding fragmentation and excessive compliance costs.

### **Recommendations for Congress**

If Congress wishes to legislate in this space, we recommend:

- Clear outcome-based standards for “highly effective” age assurance rather than prescribing specific technologies
- Explicit data minimisation and role-separation requirements
- Independent testing, audit and certification mechanisms
- Clear accountability for platforms to prevent underage use or harm coupled with safe harbour provisions for services that implement recognized standards in good faith

A comprehensive federal privacy framework would further strengthen safeguards across the ecosystem but, as we have seen at the state level, specific provisions can be included in age verification bills to prevent data retention and misuse.

### **Conclusion**

Child protection and constitutional liberties are not mutually exclusive. Carefully designed, standards-based age assurance can materially reduce minors’ exposure to age-restricted content and high-risk functionality while preserving anonymity, preventing personal data retention and respecting constitutional protections.

We would welcome the opportunity to brief the Committee on the current state of privacy-preserving age assurance technologies and relevant international standards.

Respectfully,

Iain Corby

Executive Director  
Age Verification Providers Association