

General Law Committee  
Connecticut General Assembly  
State Capitol  
Hartford  
Connecticut 06106-1562

February 18, 2026

Dear Chair Maroney, Chair Lemar and Members of the Committee,

### **HB 05037 - Written Evidence**

We are the global trade association representing 35 suppliers of privacy-preserving, anonymous, standards-based online age verification and age estimation technology solutions. We are grateful for the opportunity to submit written evidence to inform your consideration of HB 5037 which aims to promote the safety of minors on social media, expanding on the points made verbally to the Committee at its hearing today.

We are politically neutral so make no recommendation as to whether Connecticut should limit access to social media platforms, or restrict the functionality made available, to minors. But we hope to assist the Committee in its understanding of the state-of-the-art technology that allows users to quickly prove their age without disclosing their identity, and to offer some detailed comments on the current draft.

### **Response to critics**

HB 5037 can be implemented without placing sensitive personal data at risk. The bill does not require platforms to collect or retain government-issued identification, nor does it mandate centralised databases of user identity. Modern age assurance systems are typically delivered by independent third-party providers operating separately from the platforms being accessed. These providers return only a minimum age status assertion, for example that a user is “18 or older” or “not a covered minor”, without disclosing a date of birth or identity to the platform. The data used to perform the age check is deleted immediately after the attempt, consistent with the bill’s own strict minimisation requirements.

Users who are treated as minors under the bill do not need to provide any data or identity documentation. A platform may simply rely on user declaration and apply the required minor protections. In that scenario, no sensitive identity data is required from any minor at all. Where parental consent is used, the bill does not require the processing of more information than is already routinely used to comply with the Children’s Online Privacy Protection Act (COPPA). The minor need only provide contact details for a parent or guardian. The adult providing consent may be required to demonstrate that they are over 18, but this verification can likewise be conducted through independent age assurance providers that return only a binary age confirmation and do not share

identity data with the platform. Limited retention of minimal information may be necessary to allow a parent later to withdraw consent, but this is a familiar compliance model under existing federal law.

Concerns have been raised that age-verification mandates inherently undermine privacy or require biometric databases. HB 5037 does not mandate any specific method of age determination. It is technology-neutral and compatible with credential-based or document-based verification systems that do not require facial age estimation, biometric storage or government-issued ID retention. The bill expressly restricts secondary use and requires deletion after the age-check attempt. It does not require retroactive identity documentation to be stored in platform databases. Where facial age estimation tools are used, it can even be performed entirely on the user's device, so the image on which it is based never even leaves the palm of their hand.

The bill does not regulate the content of speech. It regulates a specific functionality: the personalised recommendation, selection or prioritisation of user-generated media based on information persistently associated with a user or device. Chronological feeds, search functions, direct communications and user-requested content remain available. The bill does not compel platforms to carry any speech, nor does it prohibit the removal of any speech. It targets a product feature rather than viewpoints or expressive content.

To the extent any claim is made that the bill incidentally burdens speech, Supreme Court precedent recognises that age-gating measures designed to protect minors are not automatically subject to strict scrutiny. In *Free Speech Coalition v. Paxton*, the Court confirmed that age-gating measures aimed at protecting minors may be evaluated under intermediate scrutiny, even where adults experience incidental burdens. HB 5037 is directed at protecting minors through age-based functionality limits rather than suppressing particular ideas or viewpoints.

Several early state laws have been enjoined by lower courts. In those cases, it was argued successfully that the statutes imposed broad content-based prohibitions or access restrictions to entire categories of protected speech. HB 5037 is materially narrower. It does not ban access to lawful content, does not impose viewpoint neutrality and does not require platforms to host speech they would otherwise remove.

Finally, concerns have been raised that platforms may respond by denying service to minors entirely. The bill does not require such action. It permits continued access with adjusted functionality and parental consent pathways. Decisions to withdraw services would be business choices rather than statutory mandates. None of the ten leading social media sites required by the Australian Government to restrict use to those 16 or older withdrew their services from that country – they all claim to be complying with new law.

### **Potential improvements to the text**

**“Covered User” – “In this state”** - It is important to be specific about who is subject to the provisions of this law in terms of geography. The Committee should note this has been a point of ambiguity in other states where VPNs have been seen as excusing platforms from compliance.

The Committee may want to make it clearer that the statute is not intended to allow in-state users with virtual private networks (VPNs) to circumvent the provisions. (It may be helpful to make this

point explicit in an amendment which clarifies that “social media platforms cannot rely solely on IP addresses to determine that any user is not currently in Connecticut.”)

**“(A) (i) The covered operator has used commercially reasonable and technically feasible methods to determine that the covered user is not a covered minor”**

We strongly endorse this approach to the drafting as it allows for a wide range of consumer choice in methods of age assurance.

‘**technically feasible**’ may be redundant because any option which was not technically feasible could not be commercially reasonable. It may be better to say “has used a highly effective method of age assurance, given commercially available technology”

**(i) No information that is collected for the purpose of determining a covered user's age under this subsection shall be used for any other purpose, and such information shall be deleted immediately after an attempt is made to determine the covered user's age; and**

This is an important clause which we support in jurisdictions where there is not already a strong data protection regime. If privacy / anonymity is still a concern, the Committee may wish to upgrade the requirement to ensure users are offered at least one method which is “double blind”. This, based on work by the French regulator CNIL, uses cryptography to guarantee the user cannot be identified by the platform and the age verification provider does not know which platform the user is accessing.

**(2) (A) Except as provided in subparagraph (B) of this subdivision, a covered operator that has used commercially reasonable and technically feasible methods to determine a covered user's age and is unable to determine whether the covered user is a covered minor shall presume that such covered user is not a covered minor for the purposes of this subsection.**

We urge the Committee to redraft this clause because it creates a strong incentive for minimal verification deployment and will likely undermine the intended child-safety outcome. The presumption should be reversed, protecting all users in case they are children until a commercially reasonable and highly effective method of age assurance has concluded the user is an adult.

**(ii) No information that is collected for the purpose of obtaining verifiable consent from a covered minor's parent or legal guardian shall be used for any other purpose, and such information shall be deleted immediately after an attempt is made to obtain such verifiable consent.**

This is problematic if you wish to retain the right for the parent to withdraw parental consent. A minimum dataset is required for that so the consenting parent can return to the platform, be uniquely recognised, and then withdraw that consent.

**(B) Any information that is collected for any purpose set forth in subparagraph (A) of this subdivision may be used or retained if such use or retention is necessary to comply with any federal law or regulation or any other law or regulation of this state.**

This may address the issue where another applicable law (such as COPPA) requires limited retention – but the Committee may wish to seek further legal advice to avoid confusion or conflict with the previous prohibition on any data retention. Parental-consent mechanisms may require

limited retention of minimal data, which can be designed to preserve strong privacy protections while enabling withdrawal of consent.

**"The Surgeon General has warned that while social media may have benefits for some young users, social media is associated with significant mental health harms and has not been proven safe for young users."**

This may invite a constitutional challenge as "compelled speech". That may not be fatal to the whole bill: A federal court preliminarily enjoined Colorado's social-media warning-label provisions on First Amendment compelled-speech grounds while leaving the remaining provisions of the Act in force. The addition of a severability clause would be sensible.

**(e) Not later than March 1, 2028, and annually thereafter, each covered operator shall publicly disclose, in a form and manner prescribed by the Attorney General, the following information for the preceding calendar year:**

While not of direct concern to our own members, we wonder if this will create commercial / competition concerns for their clients, with platforms required to disclose "publicly" such core management information, even if they are not publicly listed companies.

We hope our comments to the Committee and this further detail is of use, and we are, of course, available to provide further input to your deliberations.

Yours sincerely

*Iain M. Corby*

**Iain Corby**  
Executive Director