United States Internet Preservation Society
1750 Pennsylvania Ave NW #27009
Washington, DC 20006
moon@usips.org | usips.org

April 16, 2026

To the Members of the United States House of Representatives

Committee on Energy and Commerce

Re: Opposition to H.R. 8250 (“Parents Decide Act”) and to all legislation mandating operating-system-level age verification

Dear Representative:

The United States Internet Preservation Society writes to oppose H.R. 8250 and to urge Congress to reject any legislation that imposes age verification obligations on operating system providers, device manufacturers, app stores, or platform operators. Such mandates do not protect children. They compromise the privacy of every American who uses a computer, phone, tablet, console, or connected device.

A Federal Mandate for Mass Identity Exposure

H.R. 8250 would require every operating system provider to collect each user’s date of birth and to expose that date of birth to any application on the device through a mandatory programmatic interface. This is not parental control. It is a federal mandate that every general-purpose computing device in America become an identity broker for every piece of software running on it, including web browsers.

The privacy harm is severe and well-documented. In 1997, Dr. Latanya Sweeney of Carnegie Mellon University demonstrated that three data points, *date of birth, ZIP code, and sex*, are sufficient to uniquely identify 87 percent of the United States population. Date of birth is not an innocuous field on a form. It is the single most useful input to re-identification attacks, and it is the primary reason data brokers are able to correlate user activity across unrelated services. H.R. 8250 would render this data point universally available to every application on every covered device by statutory mandate.

The Mandate Applies to Every User, Not Only Minors

Section 2(a)(1) requires date-of-birth collection from all users. Section 2(a)(3) requires that the collected data be accessible to application developers. Neither provision is limited to minors. The stated child-safety purpose of the bill does not match the scope of the infrastructure it creates. Every adult, every senior citizen, every user of any covered device would be required to surrender their date of birth as a condition of using their own property, and every application on that device would gain access to that data through a federally mandated interface.

The Bill Constructs a Nationwide Fingerprinting Infrastructure

Once operating systems expose date of birth through an API, web browsers will surface that data to websites through subsequent platform interfaces. This is the consistent historical pattern for OS-level identity signals, including the Battery Status API, Device Memory API, User-Agent Client Hints, and similar surfaces. Advertisers, data brokers, and tracking networks will incorporate date of birth into their fingerprinting systems, and the resulting profiles will be dramatically more durable and more identifying than anything currently possible.

The FTC's rulemaking authority under Section 2(d)(1)(B) extends only to the manner in which operating systems collect and store the data. It does not constrain what downstream application developers do with it. H.R. 8250 does not reduce surveillance of Americans online. It industrializes it.

The Definitions Are Impermissibly Vague

H.R. 8250 defines "operating system provider" as any person who "develops, licenses, or controls" an operating system on a "general purpose computing device." Neither "general purpose computing device" nor any comparable scope term is defined anywhere in the bill. On its face, the text reaches volunteer maintainers of free software operating systems such as Debian and Ubuntu, hobbyist developers, corporate IT teams deploying internal images, smart televisions, game consoles, automotive infotainment systems, e-readers, smart watches, and embedded devices ranging from thermostats to garage door openers. No size threshold, commercial carve-out, or open-source exemption appears in the text.

Congress cannot properly delegate to an agency the foundational question of which consumer products are subject to a federal mandate backed by FTC enforcement. The regulated class must be named in the statute, not gestured at through an undefined phrase.

The "Safe Harbor" Is Not a Safe Harbor

Section 2(b) provides that an operating system provider is not liable for violating the Act if it complies with the Act. This is a definition, not a protection. It offers no shield against state privacy tort claims, state data breach statutes, consumer privacy laws such as the California Consumer Privacy Act, or biometric information laws. The bill forces the creation of a massive national database of identifying information while providing no corresponding immunity for the harms that database will inevitably cause when it is breached, and it will be breached.

The Parent-Verification Requirement Is Recursive

Section 2(a)(2) requires a parent or legal guardian to verify a minor's date of birth. Section 2(d)(1)(A)(i) defers the question of how to verify the parent's identity to FTC rulemaking. The statute itself provides no base case. Every workable answer the FTC might adopt requires either government-issued identification or a private identity-verification broker interposed between every American family and their own devices. Either outcome represents a new and permanent surveillance layer that did not previously exist.

A Less Harmful Approach Was Available and Rejected

California's AB 1043, whatever its other defects, attempts to limit privacy harm by returning age-bracket tokens rather than raw dates of birth. H.R. 8250 rejects even this minimal accommodation. Signed, non-replayable age-bracket tokens would satisfy the bill's stated child-safety purpose without exposing the underlying identifying data to every application on the device. That Congress was presented with this less harmful alternative and chose the more invasive design suggests the bill has not received the scrutiny this subject requires.

The Principle Extends Beyond H.R. 8250

USIPS opposes H.R. 8250 specifically. We also oppose, as a matter of principle, any legislation that places age verification responsibilities on operating system providers, device manufacturers, app stores, or platform operators. These parties are not well-positioned to verify identity. The systems they would be forced to build constitute surveillance infrastructure by construction. The resulting data flows cannot be contained to the purposes for which Congress authorizes their creation. Every age verification mandate directed at platforms or devices ultimately resolves to a universal identity check imposed on the entire American public, including adults with no relationship to the concerns the legislation claims to address.

The appropriate response to concerns about minors' access to online content is direct engagement with the specific content providers whose services raise those concerns, on terms that preserve user anonymity and adult access, not the conscription of every computing device in America into a federal identity verification system.

Request

The Society respectfully requests that you:

- Oppose H.R. 8250 in committee and on the floor.
- Decline to co-sponsor any successor legislation that imposes age verification obligations on operating system providers, device manufacturers, app stores, or platform operators.
- Support, as an alternative framework, legislation that provides parents with voluntary control tooling and targets specific content providers directly, without mandating universal identity collection at the operating system or device level.

The United States Internet Preservation Society remains available to discuss these issues with your office at any time. Correspondence may be directed to the undersigned.

Respectfully,

Joshua Moon
President and Treasurer

United States Internet Preservation Society

moon@usips.org