

March 12, 2025

Chair Swearingen, Vice-Chair Green, and Honorable Members of the Assembly Committee on State Affairs:

The American Civil Liberties Union of Wisconsin appreciates the opportunity to provide testimony in opposition to Assembly Bill 105.

Put simply, AB-105 raises significant concerns around privacy, surveillance, and the First Amendment. While the ACLU of Wisconsin is sympathetic to the overarching goal of this legislation, we do not believe an appropriate trade-off is compromising the civil liberties of all Wisconsinites.

AB-105 proposes to “card” all people who access websites with content deemed “material harmful to minors.” Under the bill, age verification could be conducted by checking a website-user’s government-issued identification card or “by using any commercially reasonable method that uses public or private transactional data gathered about the individual.”

The language in AB-105 bears a striking resemblance to a law passed in Texas¹ that has been challenged in federal court on First Amendment grounds.² A similar age-verification law aimed at social-media platforms passed in Arkansas was enjoined following a lawsuit challenging the law’s constitutionality.³ In enjoining each of these laws, federal courts in Texas and Arkansas found that the laws unconstitutionally discriminated against protected speech and impermissibly placed speech behind age verification requirements for both minors and adults.⁴ The Fifth Circuit Court of Appeals vacated the injunction regarding the age verification portion of the Texas law and affirmed the injunction as to a different portion of the Texas statute,⁵ and the U.S. Supreme Court granted a petition for a writ of certiorari and heard oral argument in January 2025 on the issue of whether the Fifth Circuit erred as a matter of law in applying rational-basis review, instead of strict scrutiny, to a law burdening adults’ access to protected speech.⁶

¹ Texas H.B. 1181, <https://capitol.texas.gov/tlodocs/88R/billtext/html/HB01181H.htm>.

² *Free Speech Coalition, Inc. v. Colmenero*, 689 F.Supp.3d 373 (W.D. Tex. Aug. 31, 2023).

³ *NetChoice, LLC v. Griffin*, No. 5:23-CV-05105, 2023 WL 5660155 (W.D. Ark. Aug. 31, 2023).

⁴ The two decisions followed long-established protections for speech online. Social media’s primary purpose is to allow users to speak, and “to foreclose access to social media altogether is to prevent the user from engaging in the legitimate exercise of First Amendment rights.” *Packingham v. North Carolina*, 582 U.S. 98, 108 (2017). The Supreme Court has been adamant that children “are entitled to a significant measure of First Amendment protection, and only in relatively narrow and well-defined circumstances may government bar public dissemination of protected materials to them.” *Brown v. Entertainment Merchants Ass’n*, 564 U.S. 786, 794-95 (2011); accord *Tinker v. Des Moines Ind. Comm. School District*, 393 U.S. 503 (1969). Thus, broad bars to accessing speech online based on age are likely unconstitutional.

⁵ *Free Speech Coalition, Inc. v. Paxton*, 95 F.4th 263 (5th Cir. 2024).

⁶ <https://www.scotusblog.com/case-files/cases/free-speech-coalition-inc-v-paxton/>

The two decisions further recognize that the laws' preferred regulation of speech online—age verification—places impermissible barriers between adult and minor users and the right to speech by undermining their privacy. The Arkansas court recognized that age verification requires adults and minors to surrender their anonymity.⁷ The Texas District Court expressly concluded that the evidence showed that age verification technology remains intrusive of privacy, despite purported advances in the technology.⁸ Even requirements in the law that data not be retained or used for other purposes did not alleviate the chilling effect from loss of anonymity.⁹

Common age verification methods include uploading a driver's license or state ID, facial recognition technology, or private transactional data such as a credit card. These requirements could “serve as a complete block to adults who wish to access [online] material but do not” have the necessary form of identification.¹⁰ Under AB-105, that could include Wisconsinites who do not have a driver's license or other government-issued form of identification or a credit card.

While AB-105 includes a provision that entities conducting age verification may not “retain” users' “identifying information,” the bill does not prohibit transfer of that information to third party entities—including private data broker companies or the government, creating the risk of state monitoring of what kind of websites individuals visit.

For example, the issue of storage and access could be illustrated by the difference between showing an ID at a bar and uploading an ID to a website online. At a bar, the bouncer takes a quick look at the ID to verify the age without storing or holding this sensitive information. Uploading an ID to a website carries far greater privacy risks, and the fear of the consequences of data misuse from uploading an ID to a website without knowledge is enough to scare many users away from accessing this content.

⁷ “Requiring adult users to produce state-approved documentation to prove their age and/or submit to biometric age-verification testing imposes significant burdens on adult access to constitutionally protected speech and ‘discourage[s] users from accessing [the regulated] sites.’ *Reno v. American Civil Liberties Union*, 521 U.S. 844, 856 (1997). Age-verification schemes like those contemplated by Act 689 ‘are not only an additional hassle,’ but ‘they also require that website visitors forgo the anonymity otherwise available on the internet.’ *Am. Booksellers Found. v. Dean*, 342 F.3d 96, 99 (2d Cir. 2003); see also *ACLU v. Mukasey*, 534 F.3d 181, 197 (3d Cir. 2008) (finding age-verification requirements force users to ‘relinquish their anonymity to access protected speech’).”

⁸ “First, the restriction is constitutionally problematic because it deters adults' access to legal sexually explicit material, far beyond the interest of protecting minors...People may fear to transmit their personal information, and may also fear that their personal, identifying information will be collected and stored in the records of various Web sites or providers of adult identification numbers... [the] Supreme Court has disapproved of content-based restrictions that require recipients to identify themselves affirmatively before being granted access to disfavored speech.”

⁹ The Texas court said, “Defendant contests this, arguing that the chilling effect will be limited by age verification's ease and deletion of information. This argument, however, assumes that consumers will (1) know that their data is required to be deleted and (2) trust that companies will actually delete it. Both premises are dubious, and so the speech will be chilled whether or not the deletion occurs. In short, it is the deterrence that creates the injury, not the actual retention.”

¹⁰ *PSINet, Inc. v. Champan*, 362 F.3d 227, 237 (4th Cir. 2004); see also *Am. Booksellers Found.*, 342 F.3d at 99 (invalidating age verification requirement that would make “adults who do not have [the necessary form of identification] . . . unable to access those sites”).

Determining who is a minor requires collecting sensitive information from all users—information that can then be stolen and exploited even years later.¹¹ As the court noted in *ACLU v. Gonzales*, age verification deters “many users who are not willing to access information non-anonymously...from accessing the desired information.”¹² Ultimately, by forcing adults to identify themselves in this manner to access lawful, fully protected content online that may fall under the bill’s definition of “material harmful to minors,” AB-105 imposes an unconstitutional burden on adult access to protected speech. The bill’s age verification requirement will likewise burden users who do not have government identification, who wish to exercise their First Amendment right to anonymity or who are otherwise concerned about privacy and security, or whose age or identity “commercially reasonable method[s]” will fail to accurately gauge.

While the bill’s aims are geared toward protecting minors from harmful content, AB-105 exempts the search engines that are principal gateways for minors’ access to that very content. Further, website-based age verification does not address the myriad ways internet users can circumvent verification or lead to children accessing less regulated websites.

Notably, the International Centre for Missing and Exploited Children filed an amicus brief with the U.S. Supreme Court in support of the challenge to the Texas age verification law. Their argument as to why the law would not achieve legislators’ aims was three-fold:

First, it will be ineffective. Under H.B. 1181, where more than a third of a website’s content comprises “sexual material harmful to minors,” the website must implement age verification. When implemented at the website or platform level, however, age-verification systems can be avoided easily by using widely available Virtual Private Networks (“VPNs”) or private browsers, like The Onion Router (“Tor”) network. Second, meaningful enforcement of H.B. 1181 is impractical because the law cannot be enforced extraterritorially, where many websites hosting content harmful to minors are located. Third, in light of those practical realities, H.B. 1181 will cause unintended harm. Both the Tor network and offshore websites expose minors to separate risks, such as malware, trafficking, and predation. In effect, H.B. 1181’s age-verification requirement could steer minors to more harmful corners of the internet where no such access limitation exists.¹³

Courts have invalidated age verification laws, in large part because of the significant burden verification imposes on all users and the availability of less-restrictive alternatives such as policies enabling or encouraging users (or their parents) to control their own access to information, such as content-filtering device-specific software which limits minors’ access to sexual material inappropriate for them without burdening adults’ access to speech they have a right to receive. We can make the internet safer without sacrificing the privacy and constitutional rights of all Wisconsinites.

¹¹ Matt Perault, J. Scott Babwah Brennan, “To Protect Kids Online, Policymakers Must First Determine Who is a Kid,” Tech Policy Press (July 5, 2023), <https://www.techpolicy.press/to-protect-kids-online-policymakers-must-first-determine-who-is-a-kid/>.

¹² *ACLU v. Gonzales*, 478 F. Supp. 2d 775 (E.D. Pa. 2007).

¹³ https://www.supremecourt.gov/DocketPDF/23/23-1122/309948/20240516145744135_Amicus%20Brief%20--%20Free%20Speech%20Coalition%20v.%20Paxton.pdf