No. 23-1122

IN THE

# Supreme Court of the United States

FREE SPEECH COALITION, INC., ET AL.,
*Petitioners,*

v.

KEN PAXTON, ATTORNEY GENERAL OF TEXAS,
*Respondent.*

**On Writ of Certiorari to the United States Court of Appeals for the Fifth Circuit**

## BRIEF OF *AMICUS CURIAE* AGE VERIFICATION PROVIDERS ASSOCIATION SUPPORTING RESPONDENT


BRENTON H. COOPER
BAKER BOTTS L.L.P.
700 K Street, N.W.
Washington, DC 20001
(202) 639-7700

AARON M. STREETT
*Counsel of Record*
BAKER BOTTS L.L.P.
910 Louisiana Street
Houston, TX 77002
(713) 229-1234
aaron.streett@bakerbotts.com

*Counsel for Amicus Curiae*



WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D.C. 20002

TABLE OF CONTENTS

TABLE OF CONTENTS – Continued

# TABLE OF AUTHORITIES

Page

**CASES**

TABLE OF AUTHORITIES – Continued

TABLE OF AUTHORITIES – Continued

TABLE OF AUTHORITIES – Continued

TABLE OF AUTHORITIES – Continued

IN THE

# Supreme Court of the United States

---

FREE SPEECH COALITION, INC., ET AL.,
*Petitioners,*

v.

KEN PAXTON, ATTORNEY GENERAL OF TEXAS,
*Respondent.*

---

**On Writ of Certiorari**
**to the United States Court of Appeals**
**for the Fifth Circuit**

---

## BRIEF OF *AMICUS CURIAE* AGE VERIFICATION PROVIDERS ASSOCIATION SUPPORTING RESPONDENT

---

## INTEREST OF *AMICUS CURIAE*[1]

*Amicus* Age Verification Providers Association (AVPA) is a not-for-profit global trade body representing almost 30 organizations who provide privacy-preserving, audited, and certified age-assurance solutions. Its members range from start-ups to multibillion-dollar enterprises like Experian and Fujitsu. All members must abide by AVPA's Code of Conduct, which includes requirements for protecting users' privacy in compliance with internationally recognized best practices.

AVPA members provide age-verification technology that is available to any entity that may be subject to H.B.

---

[1] In accordance with this Court's Rule 37.6, no counsel for any party has authored this brief in whole or in part, and no person or entity, other than *amicus*, their members, or their counsel, have made a monetary contribution to the preparation or submission of this brief.

1181. Contrary to the assertions of Petitioners and certain *amici*, this technology is carefully designed to protect user privacy. AVPA members' age-verification systems are already used extensively in the United States and internationally for all kinds of age-restricted purchases, from cigarettes to marijuana to gambling to pornography. AVPA members sell their services extensively in Europe, which is well known for its strict privacy regulations. AVPA members have spotless records of complying with these privacy requirements, while also providing reliable methods for purveyors of age-restricted material to verify the age of their customers.

AVPA is well acquainted with its members' age-verification systems, and it submits this brief in support of Respondent to explain the way this technology functions and to highlight the legal implications that follow from those practical realities.

## SUMMARY OF ARGUMENT

Petitioners and their *amici* contend that H.B. 1181 burdens adults' free-speech rights because it threatens user privacy and prevents undocumented users from accessing the regulated material. These arguments contradict the reality of current age-verification technology.

AVPA's members provide effective age-verification systems with robust privacy protections that allow users to access regulated material with no more privacy risk than they would experience during an in-person age check. Many of those systems use information that is *less* personally identifying than an in-person interaction, and others effectively use the same information considered during an in-person age check. What is more, user information is never shared with adult sites or anyone else and is protected from external security risks. When an AVPA member's system communicates with an adult site, it communicates *only* whether the user attempting to access

the site is over 18; any other information shared between the user and the adult site is the same information that would be shared in the absence of an age-verification requirement. Even if a data breach revealed who had used an AVPA-member system—despite the layers of security preventing such a breach—it would reveal only that the user verified his or her age, not the purpose for the age check, which can be used for many activities other than accessing pornography.

AVPA members' technology has been rigorously market-tested, including in Europe, which is renowned for its strict privacy laws. AVPA members' technology is readily available in Texas, and each system identified in this brief qualifies as a permissible age-verification method under H.B. 1181.

Because this new technology has made age-restricted internet access to pornography no more privacy-invasive than access in the analog world of *Ginsberg* v. *New York*, 390 U.S. 629 (1968), rational basis is appropriate here for the same reasons that it was in *Ginsberg*. See *Moody* v. *NetChoice*, 144 S. Ct. 2383, 2393 (2024) (explaining that First Amendment principles "do[] not change because the [interaction] has gone from the physical to the virtual world"). This technology developed in the decades since *Ashcroft* v. *ACLU* (*Ashcroft II*), 542 U.S. 656 (2004), rendering obsolete that opinion's observations about adult-speech burdens and the attendant application of strict scrutiny. However, even if strict scrutiny applied, H.B. 1181 passes muster. Petitioners and their *amici* insist that the content-filtering technology identified in *Ashcroft II* remains the least-restrictive means of ensuring children's safety online. But that rationale expired long ago because current age-verification technology protects children more effectively than content filtering—which has failed miserably at protecting children from pornography

in the twenty years since *Ashcroft II*—at negligible cost to adults' privacy.

## ARGUMENT

### I. AVPA Members Provide Privacy-Protecting, Market-Tested Age-Verification Systems That Are Readily Available In Texas And Comply With H.B. 1181

Petitioners assert H.B. 1181 imposes two burdens on adults' free-speech rights. First, Petitioners contend that "[s]ubmitting identifying information online entails risks of 'inadvertent disclosures, leaks, or hacks,' all of which are heightened because the disclosure of personal information here could 'reveal intimate desires and preferences.'" Pet. Br. 26 (quoting Pet. App. 125a-126a). Second, Petitioners allege that "'Texans who do not possess government identification or whose age or identity are not reliably confirmed by commercial age-verification systems will be functionally prohibited from visiting sites' subject to the law." *Id.* at 27 (quoting Found. for Individual Rights & Expression (FIRE) Cert. *Amicus* Br. 8).

The facts contradict these claims. As explained below, AVPA members provide age-verification systems that present an even lower risk of "reveal[ing] intimate desires and preferences" than verifying age in person at a brick-and-mortar store. *Id.* at 26. Many of those age-verification systems do not require government identification, allowing even Texans without identification to verify their age with ease.

Some *amici* who warn of these burdens do not seriously evaluate the relevant technology. FIRE, for example, baldly speculates that those who "harbor concerns about the privacy and security of state-mandated age-verification" effectively "face a * * * bar" to access the material covered by H.B. 1181. FIRE Br. 11. But "harbor[ing]

concerns" surely cannot invalidate a law when those concerns lack footing in the real world. Other *amici* purport to address the technology but overlook or misunderstand key aspects of it. See Ctr. for Democracy & Tech. Br. 7-29.

AVPA corrects the record here with its firsthand experience of market-tested, privacy-protecting age-verification systems. Each of the systems discussed in this brief is readily available in Texas and qualifies as a permissible age-verification method under H.B. 1181.

### A. With the systems offered by AVPA members, users can verify their age with less privacy risk than they would encounter when verifying their age for in-person purchases

Any time someone engages in person in an activity that requires age verification—buying cigarettes or alcohol, gambling at a casino, or even voting—there is a risk to the purchaser's privacy. If the store clerk, casino bouncer, or poll official cannot visually confirm the purchaser's age, the age verifier typically must ask for government-issued identification. That identification reveals not only the customer's age, but also his name, date of birth, address, and often even height and weight. Of course, the age checker also knows that the customer is engaging in the age-restricted activity. Depending on store policies or laws governing the sharing or storing of this information, the customer also faces the risk that this revealing data will be exposed to others. Even so, this Court routinely upholds in-person identification requirements to engage in constitutionally protected activities, without applying heightened scrutiny. See *Crawford* v. *Marion County*, 553 U.S. 181, 204 (2008) (upholding voter-identification requirement); *Ginsberg*, 390 U.S. at 643 (upholding prohibition on in-person purchase of adult "girlie" magazines by minors).

AVPA members offer many systems that allow internet users to verify their age with less privacy risk than the familiar in-person method. This becomes apparent when one examines precisely how these systems work. When a person visits an age-restricted website, the site typically offers consumers their choice of age-verification method. J.A. 186. As explained below, there are many systems for customers to choose from that closely mirror in-person age checks. This maximizes inclusivity, with options suitable for those who are not "digital natives."

### 1. Many age-verification systems do not require the user to submit any meaningful personally identifying information, while others require effectively the same data as an in-person age check

Many AVPA-member systems do not require personally identifying information at all. AVPA member Needemand offers BorderAge, which is an AI-based age-verification solution that ensures 100 percent web-user privacy. AVPA, *Needemand*.[2] With BorderAge, a user verifies his age simply by making three moves with his hands or forearms in front of his device's camera. *Ibid.* In just a few seconds, age verification is completed without the disclosure of any personally identifying information. *Ibid.* BorderAge constrains the image to 96 pixels per inch, preventing any capture of fingerprints, and if the system detects a facial feature in the frame, the age-verification stops, and the user is directed to move his face away. *Ibid.*

Another AVPA member, Privately, offers age verification that relies solely on a user's voice. Privately's VoiceAssure system employs an algorithm that analyzes a user's voice recording to confidently estimate his age

[2] https://avpassociation.com/member/needemand/

range. Privately, *VoiceAssure*.[3] A demo on Privately's website illustrates how this system works. Privately, *Privately Showroom: Age Estimation with Voice*.[4] The system instructs the user to read a given sentence into his device's microphone. *Ibid.* VoiceAssure uses "[a]dvanced algorithms" and "multiple vocal checks" to confirm that the user is over a certain age. *VoiceAssure*, *supra* note 3.[5] The system also implements anti-spoofing technology to ensure that the voice is genuine. AVPA, *Privately*.[6] A third party could trace this voice input back to a particular person only if that third party already had a link between the person and his voice. Thus, this system, like BorderAge, requires no personally identifying information as an input.

Other AVPA systems rely on personally identifying information but involve no more information than would be required by traditional in-person age verification. For example, Privately offers a "facial age estimation" tool. With this method, the "[c]ustomer's face is scanned via the device camera and [the user's] age is instantly and accurately estimated based on facial structure." Privately, *Multi-Modal Age Verification*.[7] This is functionally no different from a store clerk's immediately recognizing that a customer is well over 18 years old. In fact, Privately is less invasive than an in-person check because its algorithm analyzes only specific points and features of the face that will reveal the user's age with confidence. Just as in-person age checks can sometimes consist of nothing more than a quick glance at the customer's face, Privately's system does not require a name, email address, or anything

---

[3] https://documentation.privately.eu/guides/voiceassure
[4] https://showroom.privately.swiss/audio_recording
[5] https://documentation.privately.eu/guides/voiceassure
[6] https://avpassociation.com/member/privately/
[7] https://www.privately.eu/solutions/multi-modal-age-estimation

else. And just like its in-person counterpart, this system does not retain a copy of the user's image.

Several other AVPA members, including Yoti, offer similar age-verification products that rely on "selfies." *E.g.*, Yoti, *Everything You Need to Know About Our Facial Age Estimation Technology*.[8] This method of age verification is popular: Meta has reported that "81% of people presented with [Meta's] menu of options" to verify their age for Facebook Dating "chose to use Yoti's video selfie to verify their age." Erica Finkle, *Bringing Age Verification to Facebook Dating*, Meta (Dec. 5, 2022).[9]

Of course, just as with in-person age verification, online users also have the option of establishing their age through a government-issued identification. Twenty-two AVPA members offer such systems. See AVPA, *Overview of Members' Services*.[10] With this method, a user takes a photograph of her driver's license or passport, as well as a photograph of her face. After checking the age on the identification, matching the identification's photograph to the user, and confirming that neither image is fraudulent, the systems verify the user's age. Yoti implements a variation of this method by employing a check of a government-issued identification on the front end and then allowing users to store their ID in a virtual wallet. The information is encrypted, scrambled into "meaningless strings of numbers and letters" that can be unscrambled only with a key that is stored locally on the user's phone, and not on Yoti's servers. Yoti, *Our Approach to Security and Privacy*.[11]

---

[8] https://www.yoti.com/blog/facial-age-estimation-faq-frequently-asked-questions/

[9] https://about.fb.com/news/2022/12/facebook-dating-age-verification/

[10] https://avpassociation.com/find-an-av-provider/

[11] https://www.yoti.com/blog/our-approach-to-security-and-privacy/

### 2. All AVPA members protect user information from disclosure by the age-verification provider and from theft by malicious third parties

As standard practice, AVPA members immediately delete any user information once the verification is complete. The only exception is when jurisdictions require or incentivize retention of this information, such as when an entity retains the information pursuant to a litigation hold to prevent discovery sanctions in future litigation, or when required by Know Your Customer regulations. See, *e.g.*, 31 C.F.R. § 1020.220 (imposing customer-identification requirements for banks under the Bank Secrecy Act). Of course, in Texas, age-verification providers are flatly prohibited from "retain[ing] any identifying information of the individual." Tex. Civ. Prac. & Rem. Code § 129B.002(b).

Because the information used for age verification is immediately and permanently deleted once the check is complete, AVPA members do not share this information with adult sites that the user visits. And in the brief moments that the age-verification provider receives and processes user data, the information is protected with market-leading, bank-grade security protocols that have been developed by the PCI Security Standards Council. PCI Sec. Standards Council, *PCI Security Standards Overview*.[12]

Even in jurisdictions where AVPA members must retain this information to comply with a legal requirement, it is never shared with adult sites. That is because AVPA members must ensure that their technology is "age-aware—not identity-aware." AVPA, *Privacy: A Foundational Concept for Age Verification*.[13] Consider

---

[12] https://www.pcisecuritystandards.org/standards/

[13] https://avpassociation.com/thought-leadership/privacy-a-foundational-concept-for-age-verification/

Privately's selfie-based age-verification system. After a user verifies her age through this system, Privately immediately and permanently deletes the data-point profile of her face and retains only the fact that she is over 18 years old. When she then visits an adult site, Privately communicates to the site only that the user attempting to visit is 18 or older. Privately does not share the user's name or any other information.

This separation of powers is similar to what happens at a bar whose bouncer checks drivers' licenses at the door so that the bartender can freely serve anyone who has been allowed to enter. The bouncer might temporarily know the patron's name—just as the age-verification system temporarily knows the information the user provides. But the bartender knows only that the patron is over 18, just as an adult site knows only that the user is an adult because Privately, its "bouncer," told it so.

For this reason, the Center for Democracy and Technology misses the mark by asserting that when government-issued identifications are "paired with an individual's sensitive website visits, [the] data becomes a target for crimes such as extortion." Ctr. for Democracy & Tech. Br. 13. That is because government-issued identifications are never "paired" with a visit to an adult website. Similarly, the Center complains that it is dangerous to "link[] individuals' biometric scans to their browsing activity." *Id.* at 6. But, again, these separate pieces of information are never "linked" under the standard practices employed by AVPA members.

AVPA-member systems all operate in this fashion. For example, AVPA member VerifyMy offers a system called VerifyMyAge that allows a user to enter her email address, confirm ownership of that address with a one-time passcode, and give permission to the VerifyMyAge system to analyze online interactions and transactions that might

prove the user to be an adult—*e.g.*, taking out a mortgage or opening a credit card. VerifyMy, *Age Estimation Using Your Email Address*.[14] VerifyMy ensures that a user's "email address [is] deleted as soon as the age check is completed." *Ibid.* It is thus never shared with an adult site. Similarly, BlueCheck, a Texas-based member, can verify a user's mobile-phone number and birth date against commercially available databases commonly used for identity-verification purposes. BlueCheck, *Phone Based Age Verification*.[15] The user's information is not shared with any adult site.

Some AVPA-member systems never gain access to the personally identifying information in the first place. For example, OneID allows a user to log on to his online bank account and give the bank permission to confirm only his date of birth to the third-party age verification provider. See AVPA, *OneID*.[16] OneID does not receive access to the bank account or even the name of the account holder. The bank simply communicates to the age-verification provider that the user is 18 or older.

Likewise, Privately's systems can be structured to operate 100 percent locally on a user's device. The user's image or voice verification never leaves the palm of his hand, and the age check occurs on his device. Once complete, the device communicates to Privately's servers only that the age check has been passed. Privately then forwards this information to the adult site. Accordingly, because AVPA members do not retain personally identifying information, there is nothing for a would-be attacker to "steal" even if the member's servers were breached.

Whatever mechanism they use, AVPA members' commitment to "age aware, not identity aware" principles

---

[14] https://verifymyage.com/email-address-age-estimation
[15] https://docs.bluecheck.me/phone-based-age-verification
[16] https://avpassociation.com/member/oneid/

flows directly from AVPA's Code of Conduct, which members must follow to remain in good standing. The Code of Conduct provides that "[d]ata privacy should be paramount" and that "[m]embers should follow 'privacy and security by design' principles and make all reasonable endeavours to minimize the use and retention of personal data and to maintain the security of processed or stored personal data." AVPA, *Code of Conduct*.[17] In particular, "[m]embers should normally comply with applicable published international or local information security standards where these have been endorsed by the AVPA." *Ibid.*

One of the governing international standards specifically referenced in the Code of Conduct is ISO/IEC 27001. *Ibid.* This standard, developed by the International Organization for Standardization, "is the world's best-known standard for information security management systems" and "defines requirements an [information security management system] must meet." Int'l Org. for Standardization, *ISO/IEC 27001:2022*.[18] AVPA's Code of Conduct also requires adherence to European data-privacy laws, which are discussed in detail below. By implementing "age aware, not identity aware" principles, immediately deleting any identifying information, and deploying bank-grade security in the few moments when information is processed for age verification, AVPA members ensure close adherence to these standards. The Center for Democracy and Technology's suggestion that providers might transmit or sell personally identifying information obtained during age verification is therefore wholly unwarranted. Ctr. for Democracy & Tech. Br. 14-15.

Finally, the security of AVPA-member systems is not compromised by the user's ability to reuse an age

---

[17] https://avpassociation.com/membership/avpa-code-of-conduct/

[18] https://www.iso.org/standard/27001

verification. For some AVPA-member systems, if a user visits an adult site within a web browser after age verifying, the adult site may, typically with the user's permission, apply a cookie to the browser recording that the age-verification requirement has been met. Platforms such as Yoti store the age verification in encrypted form, with the only key stored locally on the user's phone. *Our Approach to Security and Privacy*, *supra* note 11. Other platforms such as AgeChecked allow a user to create an account on an app with a username and password, neither of which must be personally identifying. As the user visits multiple adult sites, those sites communicate with the app, which in turn communicates to the sites that an age verification has previously been completed.

In every instance, AVPA members carefully design their technology to ensure that no personally identifying information is shared with adult sites or any other third party. And AVPA members have implemented mechanisms that prevent external would-be attackers from accessing any information that is processed through the age-verification system.

**3. The age-verification process does not share any information with the adult site that would not be shared in the absence of age verification**

AVPA-member systems do not increase a user's privacy risk beyond what would be present without age verification. The age-verification process begins when the user accesses the adult site. When this occurs, the adult site creates a session identifier for the user. This identifier may allow the adult site to view the user's IP address. Upon reaching the adult site, the site then directs the user to verify his age through a third party and typically allows the user to select his method of age verification. J.A.186. The third-party age-verification system communicates

with the adult site about only one topic: whether the user attempting to access the site is 18 years of age or older.

In other words, to verify age the user accesses the adult site in exactly the same way he would without age verification. To the extent his device shares information with the adult site—such as an IP address that could potentially reveal his location—that risk stems from visiting the adult site, not any age-verification process. Requiring age verification adds only one piece of information communicated to the adult site: the user's age or age range, and nothing more.

What is more, because some Petitioners offer subscription-based websites, many of their customers have already volunteered sensitive credit-card information and email addresses to the adult site. Resp. Br. 44 (citing ROA.250-251). Age-verification systems add nothing to the privacy risks assumed by these customers.

**4. Disclosure that a particular person used an age-verification system would not reveal the purpose for which age verification was requested**

While it is highly unlikely—given the multi-layered security in place—that an identified user could be tied to a particular age-verification system, such a disclosure would not reveal the purpose for which age verification was requested. AVPA members' technology is used for a wide variety of age-restricted purchases. Among other purposes, this technology may be used to:

- make online purchases of beer or wine, see AVPA, *FAQs: What Standard of Age-Verification for Online Alcohol Sales Is Required in the UK?*;[19]

[19] https://avpassociation.com/introduction/faqs-for-consumers/

- satisfy age requirements imposed by social-media companies, see AVPA, *Age Restrictions—Advice by Sector*;[20]
- satisfy legal or platform-specific age requirements for a dating site, *ibid.*;
- make online purchases of knives or other weapons, *ibid.*;
- make online purchases of cannabis, *ibid.*;
- participate in online gambling, *ibid.*; and
- make online purchases of vaping devices, *ibid.*

Given the diverse purposes for which AVPA members' systems are used, the unlikely disclosure that a particular individual has used an age-verification system does not reveal that he did so in order to access pornography. Indeed, the disclosure risk of a user's habits is far lower than if an adult verified his age in person at an adult theatre or subscribed to pornographic websites with his credit card or email address.

### B. AVPA members offer many age-verification options for undocumented users

Petitioners worry about access for the "15 million adult citizens [who] do not have a driver's license" and the "2.6 million [who] do not have any form of government-issued photo ID." Pet Br. 27. *Amici* likewise contend that "[f]or some adults"—those without government-issued identification—the "law operates as a de facto ban." FIRE Br. 11; see also Ctr. for Democracy & Tech. Br. 11 (same).

Not so. AVPA members offer many systems that allow easy age verification without government identification. A user can display her hands, face, or voice to confirm her age. She can log on to her bank account or provide her

[20] https://avpassociation.com/age-restrictions-advice-by-sector/

mobile-phone number. Or she can share her email address to allow analysis of online transactions.

H.B. 1181 reflects this multitude of options. While it allows use of "government-issued identification" to verify age, it also allows age verification through "digital identification" or "a commercially reasonable method that relies on public or private transactional data." Tex. Civ. Prac. & Rem. Code § 129B.003. Petitioners obfuscate this point when discussing the law's alleged burden. They proclaim that age verification under H.B. 1181 is "typically [accomplished] via government-issued identification." Pet. Br. 1. The text of H.B. 1181 and the day-to-day reality of the age-verification industry show otherwise. Plus, adult sites seeking to maximize their traffic will have every incentive to offer age-verification options that are accessible by the greatest number of users.

### C. AVPA-member systems are used widely and successfully in Europe, which has strict privacy requirements

AVPA members offer their technology around the globe. Yoti alone accepts government-issued identification "from over 190 countries." Yoti, *Yoti Develops Global Code of Practice*.[21] Members have been particularly active in the United Kingdom. As just one example, businesses throughout the UK use AVPA-member technology to ensure compliance with the UK's prohibition on the sale of vaping products to customers under 18. See *The Nicotine Inhaling Products (Age of Sale and Proxy Purchasing) Regulations 2015*, SI 2015/895 (UK).[22]

AVPA-member technology is also used to comply with other European nations' age restrictions on adult content.

---

[21] https://www.yoti.com/blog/yoti-code-of-practice-for-sharing-health-data-covid-19-credentials/

[22] https://www.legislation.gov.uk/uksi/2015/895/contents

In Germany, the Protection of Young Persons Act and the Interstate Treaty on the Protection of Minors in the Media impose age restrictions on access to pornography. See Fed. Agency for Child & Youth Protection in the Media, *General Information*.[23] In France, Law No. 2020-936 authorizes the Regulatory Authority for Audiovisual and Digital Communication to block websites that do not comport with the Law's age restrictions on adult content. Libr. of Cong. Glob. Legal Monitor, *France: Parliament Adopts Law Against Domestic Violence*.[24] Adult-content providers use AVPA-member technology to comply with these laws. And in the UK, Part 5 of the UK Online Safety Act of 2023 will require "highly effective" "age verification or age estimation" by all "providers of * * * pornographic content" when it takes effect in January 2025. Online Safety Act 2023, c. 5 § 81(3) (UK).[25] Businesses are prepared to meet this requirement with the same AVPA-member technology they use to comply with UK vape-sale restrictions. These are just three international examples among many, encompassing both adult websites and other age-restricted online activities.

In Europe, AVPA members are bound by the EU General Data Protection Regulation ("GDPR"), which is the "strongest privacy and security law in the world." Council of the Eur. Union, *The General Data Protection Regulation*;[26] see also Adam Satariano, *G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. Times (May 24, 2018) (describing GDPR as the "world's toughest" set of rules "to protect people's online

---

[23] https://www.bzkj.de/bzkj/meta/en

[24] https://www.loc.gov/item/global-legal-monitor/2020-08-07/france-parliament-adopts-law-against-domestic-violence/

[25] https://www.legislation.gov.uk/ukpga/2023/50/part/5

[26] https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/

data").[27] The GDPR "establishes the general obligations of data controllers and of those processing personal data on their behalf." *The General Data Protection Regulation*, *supra* note 26. These "include the obligation to implement appropriate security measures, according to the risk involved in the data processing operations they perform." *Ibid.*

AVPA members comply with GDPR through their best-in-class data-security protocols. During the preparation of this brief, the UK Information Commissioner's Office ("ICO") confirmed to AVPA that the ICO has not taken enforcement action under the UK's own version of the GDPR or under the Children's Code—a similar privacy law that applies to children's data—against a service that uses age-estimation or age-verification methods. This strong track record disproves Petitioners' speculation about risks to anonymity.

AVPA members have thrived in the marketplace while maintaining this compliance. Worldwide, AVPA members have completed over 875 million age checks for over 30 million individuals in the last five years. AVPA members work with over 200 adult-content clients, which run over 1,000 adult websites using AVPA-member technology for age verification. Yet according to an AVPA survey, no member has reported that any adult-industry clients have ceased to operate as a result of implementing age assurance. This real-world experience powerfully confirms that age-verification technology can be used with negligible risk to privacy or adult access.

---

[27] https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html

### D. AVPA-member systems are readily available in Texas and qualify as permissible age-verification methods under H.B. 1181

AVPA members' systems are readily available in Texas. Of the twenty-eight members that offer age-verification platforms, 14 offer systems for download in Texas. That number includes all the age-verification systems referenced in this brief. These systems are also affordable. An adult site can typically complete age checks with AVPA members for approximately 12 cents per user per year, and this cost is expected to fall as age-verification technology continues to advance.

Each system mentioned in this brief is also a permissible method of age verification under H.B. 1181. The law allows three types of age verification: (1) "digital identification"; (2) a "commercial age verification system that verifies age using * * * government-issued identification"; or (3) a "commercial age verification system that verifies age using * * * a commercially reasonable method that relies on public or private transactional data to verify the age of an individual." Tex. Civ. Prac. & Rem. Code § 129B.003. AVPA members' systems that use government-issued identification plainly qualify, while others fall into the remaining two categories.

"Digital identification" is defined as "information stored on a digital network that may be accessed by a commercial entity and that serves as proof of the identity of an individual." *Id.* § 129B.003(a). "Transactional data" is defined in the statute as "a sequence of information that documents an exchange, agreement, or transfer between an individual, commercial entity, or third party used for the purpose of satisfying a request or event," "includ[ing] records from mortgage, education, and employment entities." *Id.* § 129B.001(7). These definitions are sufficiently capacious to include all the systems described in this brief.

The Fifth Circuit therefore correctly concluded that each of the age-verification systems described herein qualify as permissible methods under the statute. Pet. App. 11a.

## II. AVPA-Member Systems Are Difficult To Circumvent

Petitioners' *amici* misfire in claiming that age-verification systems like those discussed in this brief are easy to circumvent. The Center for Democracy and Technology asserts that a teenager could use someone else's identification and match it to an image of that person, or perhaps create a fake identification with the teenager's face to match with the teen's photograph. Ctr. for Democracy & Tech. Br. 10.

AVPA members have invested substantial resources into thwarting both types of workarounds by detecting fraudulent images. On the former, AVPA-member systems rigorously assess the "liveness" of the facial check, so an image of someone else will not suffice. One system obtains a series of images in quick succession to discern eye movement between each image. Independent testing found that the median system using this technology detects 99.99 percent of imposters. Maryland Test Facility, *Remote Identity Validation Technology Demonstration*.[28] On the latter workaround, AVPA-member technology can determine when a purported government-issued identification is a counterfeit. For example, Yoti employs around-the-clock security operations that rely on both artificial intelligence and skilled operatives to review government-issued documents to ensure their authenticity. In any event, an equal or greater risk of fake documentation is present when a shopkeeper verifies a customer's age by physically checking identification. *E.g.*, Amelia M. Arria *et al.*, *False*

[28] https://mdtf.org/rivtd/Results2023?Length=0

*Identification Use Among College Students Increases the Risk for Alcohol Use Disorder: Results of a Longitudinal Study*, Nat'l Inst. of Health 7 (Mar. 1, 2015) ("On average, students used false IDs during [24.1 percent] of their drinking occasions before they turned 21[.]").[29]

The Center also suggests that biometric scanning of a user's hands, voice, or face is ineffective. Ctr. for Democracy & Tech. Br. 22-26. Contrary to the Center's claim, selfie-based age-verification systems are equipped to analyze faces of all ethnicities. Yoti recently published figures showing there is "no discernible bias across genders or skin tones" for its facial age-estimation system. Yoti, *Facial Age Estimation White Paper* (Sept. 9, 2024).[30]

Moreover, while biometric age verification cannot perfectly identify a user's age, it effectively waves in the vast majority of users who are well over 18, leaving potential doubts only as to those between 18 and 21. But users in that narrow category have ample alternative methods of verifying age. And requiring a user to provide an additional source of age verification when he appears to be close to the age threshold is no different from routine in-person age checks. "Facial age estimation can be configured to work with legal age thresholds in a similar way" by, for example, requiring additional age verification for users detected to be under 21. Yoti, *Yoti Facial Age Estimation White Paper* 8 (Sept. 2024).[31] Yoti's facial-

---

[29] This manuscript is publicly available at https://pmc.ncbi.nlm.nih.gov/articles/PMC3959274/pdf/nihms519469.pdf. The article was published in final edited form in *Alcoholism: Clinical and Experimental Research*. Amelia M. Arria *et al.*, *False Identification Use Among College Students Increases the Risk for Alcohol Use Disorder: Results of a Longitudinal Study*, 38 Alcoholism: Clinical & Experimental Rsch. 834 (Mar. 2014).

[30] https://www.yoti.com/blog/yoti-age-estimation-white-paper/

[31] https://www.yoti.com/wp-content/uploads/2024/11/Yoti-Age-Estimation-White-Paper-September-2024-PUBLIC.pdf

recognition age-estimation tool correctly detects that 13 to 17 year olds are under 21 with 99.2 percent accuracy. *Id.* at 3. Thus, available techniques safeguard children while imposing only a seamless backup check on those estimated to be close to the age threshold.

Finally, the Center conjectures that a teenager may employ deepfakes or otherwise deceive the facial-recognition tool. While advanced supercomputers may have the processing power to create a deepfake that could circumvent AVPA members' sophisticated anti-spoofing checks, such technology is unlikely to be available to the average teen. See Yoti, *On the Threat of Generative AI* 6 (Feb. 2024) (detailing how Yoti "provide[s] the latest technology available to combat attempts to spoof or produce generative AI content").[32]

Tellingly, the Center conveniently ignores age-verification methods that confirm the user's date of birth through a bank. And it is difficult to imagine how such third parties could be tricked into confirming a false date of birth. While a teen could perhaps collude with an adult to bypass any age-verification system, *e.g.,* Ctr. for Democracy & Tech. Br. 10, that risk is no more prevalent online than it is in person, where an adult can always purchase alcohol, cigarettes, or pornography, and promptly transfer them to a minor.

## III. Because H.B. 1181 Does Not Meaningfully Burden Adults' Access To Speech, It Is Subject To Rational-Basis Review

H.B. 1181 is aimed at protecting children from exposure to pornography. The Fifth Circuit correctly held that rational-basis review applies so long as H.B. 1181 does not have spillover effects that meaningfully burden the right

---

[32] https://www.yoti.com/wp-content/uploads/2024/03/Yoti-How-to-combat-Generative-AI-and-deepfakes-white-paper.pdf

of adults to view the age-restricted material. After all, in *Ginsberg*, this Court applied rational-basis review to an age-restrictive New York law that allowed stores to "stock and sell" "so-called 'girlie' picture magazines" to adults, while prohibiting their sale to minors. Pet. App. 8a. *Ginsberg* thus instructs that "regulation of the distribution to minors of speech obscene for minors is subject only to rational-basis review." *Ibid.*

Petitioners do not dispute that rational-basis review applies if there are no material burdens on adult speech. They acknowledge that "the Court has uniformly held that a content-based *burden on adults' access to such protected speech* 'can stand only if it satisfies strict scrutiny.'" Pet. Br. 1 (emphasis modified) (quoting *United States* v. *Playboy Ent. Grp., Inc.*, 529 U.S. 803, 813 (2000)). Petitioners argue for strict scrutiny because, in their view, H.B. 1181 "imposes *a clear burden*, forcing *adult* users to incur severe privacy and security risks." *Id.* at 13 (emphases added).

In a First Amendment regime that differentiates between the speech rights of children and adults with respect to obscene material, the mere need to establish that one *is* an adult cannot—without more—be sufficient to trigger strict scrutiny. Cf. *Sable Commc'ns of Cal., Inc.* v. *FCC*, 492 U.S. 115, 125-126 (1989) (explaining that the state can require the speaker distinguish between audiences that have differing rights with respect to the speech); *Ashcroft* v. *ACLU* (*Ashcroft I*), 535 U.S. 564, 583 (2002) (reaffirming *Sable*). Rather, meaningful burdens on adult speech are the key to unlocking heightened scrutiny. That approach is consistent with other contexts where the Court evaluates identification requirements for the exercise of protected rights. *E.g., Crawford*, 553 U.S. at 202-203 (declining to apply strict scrutiny where the voter-identification law "impose[d] only a limited burden on voters' rights").

This Court's post-*Ginsberg* decisions confirm that age restrictions trigger strict scrutiny only if they impose material burdens on adults' ability to access protected speech. In *Reno* v. *ACLU*, the Court applied strict scrutiny to age limitations on "indecent" material contained in the Communications Decency Act of 1996 ("CDA") in part because of the "absence of a viable age verification process." 521 U.S. 844, 876 (1997). Without such a process, the CDA "effectively suppresse[d] a large amount of speech that adults have a constitutional right to receive," placing a "burden on adult speech." *Id.* at 874.

Similarly, in *United States* v. *Playboy Entertainment Group, Inc.*, strict scrutiny applied because the statute there "required cable television operators who provide channels primarily dedicated to sexually-oriented programming either to fully scramble or otherwise fully block those channels or to limit their transmission to hours when children are unlikely to be viewing." 529 U.S. 803, 806 (2000). That statute, unlike H.B. 1181, did not merely ensure that only adults could view certain speech; it facially burdened adults' right to receive speech during most of the day. *Id.* at 807. As the Fifth Circuit correctly recognized, the statute in *Playboy* "targeted distribution to all" whereas H.B. 1181 and the statute in *Ginsberg* "targeted distribution to minors." Pet. App. 21a.

Finally, *Ashcroft II* did not evaluate the proper level of scrutiny, *id.* at 16a-19a, because the parties did not dispute that the statute "was likely to burden some speech that is protected for adults." 542 U.S. at 665. As in *Reno* and *Playboy*, moreover, the statute in *Ashcroft II* imposed a greater burden on adult speech than H.B. 1181 because it was a criminal statute that merely made age verification a defense. *Id.* at 670-671. And *Ashcroft II*'s assessment of burden also rested on "[then-]current technological reality," which did not offer the same tailored and secure age-verification methods that are available today. *Id.* at 671.

The dispositive question, then, is whether H.B. 1181 materially burdens adult speech. Petitioners identify two purported burdens lurking in the age-verification provisions: First, "[s]ubmitting identifying information online entails risks of 'inadvertent disclosures, leaks, or hacks,' all of which are heightened because the disclosure of personal information here could 'reveal intimate desires and preferences.'" Pet. Br. 26 (quoting Pet. App. 125a-126a). Second, "Texans who do not possess government identification or whose age or identity are not reliably confirmed by commercial age-verification systems will be functionally prohibited from visiting sites subject to the law." *Id.* at 27 (quoting FIRE Cert. *Amicus* Br. 8).

As the foregoing discussion of AVPA members' age-verification technology illustrates, Petitioners' alleged burdens are ephemeral. The privacy and access burdens for online age verification are no greater—and arguably much lighter—than they were in the brick-and-mortar world of *Ginsberg*. No user faces a meaningful privacy risk when using AVPA members' technology, much of which does not rely on personally identifying information and all of which immediately and permanently deletes any personal information upon completing the age verification, consistent with H.B. 1181's mandate. Consequently, it is vanishingly unlikely that the age-verification requirement could ever result in public disclosure that a particular user visited an adult site. What is more, Texans without government-issued identification may verify their age using their hands, face, voice, email address, mobile-phone number, or bank account.

The contrast with cases where the Court applied strict scrutiny is striking. The statute in *Playboy* operated as a total ban on adults' access to sexually oriented television programming during certain time periods. 529 U.S. at 806. H.B. 1181 allows Texans to visit adult sites at any time, so long as they first verify their age through one of

the seamless systems offered by AVPA members. The statute in *Reno* imposed a "burden [on] communication among adults" due to "the absence of a viable age verification process." 521 U.S. at 876. H.B. 1181, by comparison, was enacted against the backdrop of a vibrant market of "viable age verification" providers who facilitate adult access to protected material every hour of every day in countries throughout the world. The change in that critical factual context leads to a different constitutional outcome.

In light of the technology offered by AVPA's members, the Fifth Circuit properly concluded that "the world of *Ginsberg* and our world" are sufficiently similar that rational-basis review applies to H.B. 1181. Pet. App. 11a. Just as the in-person milieu of *Ginsberg* protected minors while imposing fleeting, incidental burdens on adults, the same is true of H.B. 1181. Incidental burdens that inhere in proving that a person is an adult do not warrant strictly scrutinizing a state's good-faith efforts to safeguard children. The principles of *Ginsberg* "do[] not change because the [interaction] has gone from the physical to the virtual world." *NetChoice*, 144 S. Ct. at 2393.

Petitioner's attempts to inflate H.B. 1181's burdens vis-à-vis *Ginsberg* miss the mark. First, Petitioners argue that H.B. 1181 requires only that "[e]ntities conducting [] verification may not 'retain' users' 'identifying information,'" but "does not prohibit transfer of that information or impose any other protection against disclosure." Pet. Br. 1 (quoting Tex. Civ. Prac. & Rem. Code §§ 129B.002(b)). Any theoretical possibility of transfer, however, is evanescent in light of the technology described above. Some age-verification systems use little or no personally identifying information at all. For these systems, there is nothing to transfer. Some systems run the age-verification process entirely on the user's device, giving nothing to the age verifier's servers except for age confirmation. Regardless of the system, no AVPA member

transfers or discloses identifying information used for age verification; they immediately delete it. Anything else would violate AVPA's Code of Conduct and the incorporated international privacy standards and fatally damage the disclosing age verifier's reputation in the marketplace.

Second, Petitioners argue that the statute in *Ginsberg* "barred only 'knowing' sales to minors and did not prescribe age verification in any form." Pet. Br. 30. They thereby implausibly suggest that New York shopkeepers had no obligation to assess the age of their customers. But where criminal statutes "require proof that a defendant acted knowingly or willfully," the "doctrine of willful blindness hold[s] that defendants cannot escape the reach of these statutes by deliberately shielding themselves from clear evidence of critical facts that are strongly suggested by the circumstances." *Global-Tech Appliances, Inc.* v. *SEB S.A.*, 563 U.S. 754, 766 (2011). Under this doctrine, a shopkeeper could not claim ignorance of his customer's age as an excuse. In any event, Petitioners' reading of *Ginsberg* would establish at most that the *New York law* imposed very little burden on adults; it does not establish that *H.B. 1181* imposes material burdens on adult speech. Because it does not, rational-basis review applies.

## IV. H.B. 1181 Survives Any Form Of Heightened Scrutiny

If rational-basis review does not apply, AVPA agrees with Respondent that nothing more than intermediate scrutiny is appropriate. Given the advanced state of age-verification technology, H.B. 1181's incidental burdens on adult speech make it analogous to a zoning law that does not suppress speech based on its content. As Justice O'Connor recognized in *Reno*, evolving technology would one day support the application of intermediate scrutiny to online-speech regulations that differentiate between children and adults. 521 U.S. at 889-891 (O'Connor, J.,

concurring in part). That day has now arrived, and H.B. 1181 easily satisfies intermediate scrutiny for the reasons given below and in Respondent's brief.

Even if strict scrutiny applies, H.B. 1181 passes muster. Petitioners argue that H.B. 1181 flunks strict scrutiny because this Court—more than twenty years ago—believed that "content-filtering software" was then "both less restrictive and more effective" than online age verification. Pet. Br. 39 (citing *Ashcroft II*, 542 U.S. at 666-673). Whatever purchase that reasoning had in 2004, it no longer applies to today's technological environment.

For starters, content filtering is no longer as effective as age verification. Since *Ashcroft II*, content filtering has been the primary method of protecting youth from the harms associated with pornography. And yet minors' access to pornography has soared to all-time highs. In 2018, the average age of first pornography exposure was 11 years old. Byrin Romney, *Screens, Teens, and Porn Scenes: Legislative Approaches to Protecting Youth from Exposure to Pornography*, 45 Vt. L. Rev. 43, 48 & n.15 (2020) (citing Khadijah Watkins, *Impact of Pornography on Youth*, 57 J. Am. Acad. Child & Adolescent Psych. 89 (2018)). Viewers of pornography are sometimes as young as eight years old, while 72.8 percent of children have encountered pornography by age 18. Chiara Sabina, Janis Wolak, & David Finkelhor, *The Nature and Dynamics of Internet Pornography Exposure for Youth*, 11 Cyberpsych. & Behav. 691, 691-692 (2008). The *Ashcroft II*–mandated experiment with content filtering has failed miserably. Indeed, one Oxford study concluded that a "caregiver's use of Internet filtering had inconsistent and practically insignificant links with young people reports of encountering online sexual material." Andrew K. Przyblski & Victoria Nash, *Internet Filtering and Adolescent Exposure to Online Sexual Material*, 17 Cyberpsych., Behav., & Soc. Networking 405, 405 (2018).

Content filtering requires cooperation among too many different entities to be successful. In its current incarnation, content filtering first requires adult sites to apply a "Restricted to Adult" ("RTA") watermark to their entire site. RTA Label, *What Is The RTA Label?*[33] Such a labeling process, whether done manually or with the help of artificial intelligence, is likely to be either under- or overinclusive. The entity that carries out the content filtering—typically either the web browser or the device manufacturer—must then create a mechanism that prevents minors, but allows adults, to access RTA content. The system often relies on parental involvement to actively manage the divide between these two tracks. With device-level content filtering, that means parents must ensure that a device previously designated as an adult device is not borrowed or handed down to a child. And parents rarely engage content filters. In a recent Senate Judiciary Committee hearing, Snap CEO Evan Spiegel revealed that approximately 20 million U.S. teenagers use Snapchat, but only about 200,000 parents utilize its Family Center supervision controls, suggesting that only about one percent of parents implement parental-control features. Aisha Malik, *Snap CEO Says 20 Million US Teens Use Snapchat, But Only 200,000 Parents Use Its Family Center Controls*, TechCrunch (Jan. 31, 2024).[34]

By contrast, age verification enabled by AVPA-member technology imposes the obligation to prevent minors from accessing pornography solely on the adult sites themselves. That is a particularly effective place to locate this obligation because the sites are the one category of

---

[33] https://www.rtalabel.org/index.html?assets/pages/default.php#what-is-rta

[34] https://techcrunch.com/2024/01/31/snap-ceo-says-20-million-u-s-teens-use-snapchat-but-only-200000-parents-use-its-family-center-controls/

entities that knows both (1) which material is pornographic and (2) who is trying to access the site. Cf. *Sable*, 492 U.S. at 125-126 (recognizing that the state may impose gatekeeping obligations on the speaker).

This Court's decades-old case law expressing a preference for content filtering was based on then-current technology that has changed dramatically in the intervening years. In *Reno*, the Court held that the CDA's age requirements were unconstitutional given the Government's concession that there was "no effective way to determine the identity or the age of a user who is accessing material." 521 U.S. at 855. That is no longer true. Similarly, *Ashcroft II* recognized that there was a "serious gap in the evidence as to the effectiveness of filtering software." 542 U.S. at 671. The twenty years since have filled that evidentiary gap with overwhelming proof that content filtering is singularly ineffective in protecting children from pornography.

In sum, the technological assumptions that drove the strict-scrutiny outcome in *Reno* and *Ashcroft II* do not require the same result today. While our Constitution does not evolve, facts and technology do. See *Shelby County* v. *Holder*, 570 U.S. 529, 557 (2013) (invalidating Section 4 of Voting Rights Act where new facts revealed the preclearance formula was no longer tailored to prevent likely constitutional violations). And the current state of technological facts dictates that H.B. 1181 must be upheld even if strict scrutiny applies.

## CONCLUSION

AVPA respectfully requests that the Court affirm the judgment below.

Respectfully Submitted.

BRENTON H. COOPER
BAKER BOTTS L.L.P.
700 K Street, N.W.
Washington, DC 20001
(202) 639-1325

AARON M. STREETT
*Counsel of Record*
BAKER BOTTS L.L.P.
910 Louisiana St.
Houston, TX 77002
(713) 229-1234
aaron.streett@bakerbotts.com

*Counsel for Amicus Curiae*

November 2024