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 THE MANHATTAN INSTITUTE AND TECHNOLOGY SCHOLARS AS *AMICI CURIAE* IN SUPPORT OF RESPONDENT

ILYA SHAPIRO
JOHN KETCHAM
TIM ROSENBERGER
MANHATTAN INSTITUTE
52 Vanderbilt Ave.
New York, NY 10017
(212) 599-7000
ishapiro@manhattan.institute

JONATHAN BERRY
JAMES R. CONDE
Counsel of Record
ADAM H CHAN
BOYDEN GRAY PLLC
800 Connecticut Ave. NW, Suite 900
Washington, DC 20006
(202) 955-0620
jconde@boydengray.com

TABLE OF CONTENTS

INTEREST OF *AMICI CURIAE* 1

SUMMARY OF ARGUMENT 2

ARGUMENT 5

I. Age-Verification Technologies Ensure Privacy at Low Cost 5

A. Available Age-Verification Methods Protect Privacy and Cybersecurity 5

1. Zero-Knowledge Proofs 6

2. Biometric Age Verification and Estimation 8

3. Trusted Third-Party Verifiers 10

B. Age Verification Is Inexpensive 13

II. Governments Often Require Age Verification 15

III. Online Activity Isn't Private Anyway 17

IV. Age Verification Helps Even if Some Minors Evade It 20

V. Parental Controls Are More Invasive than Age Verification 22

CONCLUSION 24

TABLE OF AUTHORITIES

Page(s)

Cases

Ashcroft v. ACLU,
542 U.S. 656 (2004) 2, 5, 13, 17

Ginsberg v. New York,
390 U.S. 629 (1968) 4, 19

South Dakota v. Wayfair,
585 U.S. 162 (2018) 19

Statutes

15 U.S.C. § 1637(c)(8) 21

Credit Card Accountability
Responsibility and Disclosure Act of
2009, Pub. L. No. 111-24,
123 Stat. 1734 21

La. Stat. Ann. § 9:2800.29 10

La. Stat. Ann. § 9:2800.29(B)(2) 11, 19

Tex. Civ. Prac. & Rem. Code §
129B.002(a) 5

Other Authorities

Adam Candeub, *Online Age-Verification: Protecting Children and Privacy*, Ctr.
for Renewing Am. (July 21, 2023) 8

Age Check Users Globally from a Selfie, Yoti 9

Age Verification, Yoti 12, 13

Alexander Berentsen et al., *An Introduction to Zero-Knowledge Proofs in Blockchains and Economics*, 105 Fed. Rsrv. Bank St. Louis Rev. 280 (2023) 6

Álvaro Feal et al., *Angel or Devil? A Privacy Study of Mobile Parental Control Apps*, 2 Proc. Priv. Enhancing Tech., 314 (2020) 22

Angie Jones, *Our California DMV Hackathon Win: Privacy-Preserving Age Verification* (Oct. 15, 2024) 12

Apple, Media Statement, *The Facts About Parental Control Apps* (Apr. 28, 2019) 23

Arizona Dep't of Transp., Press Release, *Adot Mvd Offers Retailers a New App for Mobile ID Age Verification* (July 30, 2024) 14

Ash Johnson, *The Path to Digital Identity in the United States* (2024) 21

AuthenticID, Press Release, *California DMV Fortifies Mobile Driver's License (mDL) Enrollment with AuthenticID's Identity Verification Technology*, (Nov. 13, 2024) 19

Bring Digital Verification to Your Business, LA Wallet 10

Browser Fingerprinting-A Thorough Overview, fraud.com 18

Digital Capabilities for Real Time Identification, LA Wallet..... 10

DraftKings Inc., Registration Statement (Form S-1) (May 6, 2020) 15

Eric N. Holmes, Cong. Rsch. Serv., LSB11020, *Online Age Verification (Part I): Current Context* 2 (2023) 5

Erica Finkle, *Bringing Age Verification to Facebook Dating*, Meta Newsroom (Dec. 5, 2022) 13

Hackathon, Meriam-Webster Online Dictionary 12

How Do You Check Age Online?, Age Verification Providers Ass'n..... 16

How Websites and Apps Collect and Use Your Information, U.S. Fed. Trade Comm'n (Sept. 2023) 17

Jared Ronis, *Don't Trust When You Can Verify: A Primer on Zero-Knowledge Proofs*, Wilson Ctr. (Feb. 7, 2024) 6, 7, 8, 19, 20

Jean-Jacques Quisquater et al., *How to Explain Zero-Knowledge Protocols to Your Children*, 435 Lecture Notes in Comp. Sci. 628 (1989) 7

Jérôme Gorin et al., *Demonstration of a Privacy-Preserving Age Verification Process*, LINC (June 22, 2022) 8

Kavitha Cardoza, *Hackers are Targeting a Surprising Group of People: Young Public School Students*, NPR (Mar. 12, 2024) 23

Kelvin Chan, *Three of the Biggest Porn Sites Must Verify Ages to Protect Kids Under Europe's New Digital Law*, AP (Dec. 20, 2023) 16

Kevin E. Davis & Florencia Marotta-Wurgler, *Filling the Void: How E.U. Privacy Law Spills Over to the U.S.*, J.L. & Empirical Analysis 1 (2024) 17

Lauren Leffer, *Online Age Verification Laws Could Do More Harm Than Good*, Sci. Am. (Apr. 16, 2024) 20

Lauren Martinez, *Digital ID: Here's How Mobile Driver's License Tech Could Be Used by Bay Area Businesses*, ABC 7 News (Oct. 2, 2024) 11

Lorenzo Franceschi-Bicchierai, *Spyware Company Exposed '281 Gigabytes' of Children's Photos Online*, Vice (Apr. 30, 2018) 23

Manuel G. Pascual, *How Age Verification to Access Porn Works in France: 'They Won't Know Anything About You, Other Than That You're an Adult,'* El Pais English (May 7, 2024) 16

Matt Prendergast, *Age Check Certification Scheme Evaluation for Yoti Facial Age Estimation*, Yoti Blog (Oct. 25, 2024) 10

Microsoft Security, *Microsoft Entra Verified ID* (2004) 14

Reusable Age Checks, Yoti 13, 15

Smart ID Verifier App, Arizona Dep't of Transp. 14

Sup. Ct. R. 37.6 1

Suzan Ali et al., *Betrayed by the Guardian: Security and Privacy Risks of Parental Control Solutions*, *in* Procs. of the 36th Ann. Computer Sec. Applications Conf. 69 (2020) 22

Timilehin B. Aderinola et al., *Learning Age from Gait: A Survey*, 9 IEEE Access 100352 (2021) 9, 21

Using Remote Verify You / Verification, LA Wallet (Oct. 9, 2024) 11

Vignesh Krisnakumar, *How Multimodal Biometrics Help with Age Verification and Compliance*, Biometric Update (Oct. 2, 2024) 9

Zack Whittaker, *Teen Phone Monitoring App Leaked Thousands of User Passwords*, ZDNet (May 20, 2018) 23

INTEREST OF *AMICI CURIAE*[1]

Amici are:

THE MANHATTAN INSTITUTE FOR POLICY RESEARCH, a nonpartisan public policy research foundation dedicated to developing and advancing ideas that foster greater economic opportunity, individual responsibility, and adherence to the rule of law. To that end, the Manhattan Institute has sponsored scholarship and filed briefs on the need to both safeguard the well-being of children and uphold the freedom of speech.

JONATHAN ASKONAS, Assistant Professor of Politics at the Catholic University of America and Senior Fellow at the Foundation for American Innovation.

ADAM CANDEUB, Professor of Law at Michigan State University and Director of its Intellectual Property, Information, and Communications Law Program.

AARON DOMINGUEZ, Provost and Ordinary Professor of Physics at the Catholic University of America.

MEG LETA JONES, Provost's Distinguished Associate Professor in Communication, Culture, and Technology at Georgetown University.

---

[1] No counsel for any party authored this brief in whole or in part, and no person or entity other than *amici* or its counsel made a monetary contribution to fund the preparation or submission of the brief. *See* Sup. Ct. R. 37.6.

KEEGAN MCBRIDE, Lecturer in AI, Government, and Policy at the Oxford Internet Institute of the University of Oxford.

Amici have an interest in helping the Court on issues within *amici*'s expertise. Here, in particular, *amici* write to inform the Court of the burdens—in terms of expense and risk to privacy—that current age verification imposes on internet users. *Amici* all agree with Texas that age-verification technologies require little, if any, identifying information, and have a limited effect, if any, on personal privacy. Expenses, in terms of financial cost and inconvenience, are negligible.

SUMMARY OF ARGUMENT

In the two decades since the Court's decision in *Ashcroft v. ACLU*, 542 U.S. 656 (2004), age-verification technology has rapidly evolved. Today, available age-verification options can protect user privacy, minimize costs, and ensure easy access to lawful adult content, while advancing the state's interest in restricting minors' access to pornography or other harmful content. In light of these developments, the Court should revisit the assumptions it made in *Ashcroft* and affirm the Fifth Circuit's judgment under any level of scrutiny.

Amici make five key points.

First, available technologies allow websites to verify or accurately estimate that a user is at least 18 years of age without revealing other identifying information about the user. Unlike older online age-verification techniques, new methods don't need to store

sensitive personal data to verify a user's age, thus offering more security and privacy than older methods. Zero-knowledge proofs ("ZKPs"), for example, are widely used in high-privacy applications such as cryptocurrency. ZKPs are scalable and accessible, making the cost of implementing an age-verification system minimal.

Digital-identification platforms, such as Louisiana's LA Wallet, also allow users to prove their age without revealing any other identifying information to the websites they visit. LA Wallet's VerifyYou Pro ensures that only the bare minimum information—is the user over 18?—is disclosed to the website. This allows businesses to validate their customers' age quickly, easily, and cheaply. These systems therefore don't present the privacy risks the Court identified two decades ago in *Ashcroft*.

Second, age-verification technologies are commonplace in many settings, both across the United States and the developed world. Online banking, sports betting, and alcohol-delivery companies use age verification to ensure compliance with age limits. Like Texas, several European countries, and the European Union, already require firms operating pornographic websites to verify age. Firms operating pornography websites are thus increasingly familiar with age verification. If they can comply in Europe, then they can comply in Texas.

Third, age verification doesn't materially increase privacy risks. Online activity isn't private to begin with. The anonymous online experience this Court as-

sumed in *Ashcroft* has no basis in contemporary reality. Modern internet use is characterized by pervasive data collection, tracking, and profiling. Cookies, IP address monitoring, and device identifiers routinely compromise user privacy. Given today's heavily tracked online experience, modern age-verification technologies don't meaningfully compromise online privacy. Indeed, online age verification imposes fewer burdens on personal privacy than the in-person age-verification requirement this Court upheld as constitutional in *Ginsberg v. New York*, 390 U.S. 629 (1968).

Fourth, Petitioners' argument that age-verification measures may be evaded by crafty minors—using virtual private networks ("VPNs") or stolen credentials—makes perfect the enemy of the good. Although no system is foolproof, age-verification technologies will meaningfully reduce the number of minors accessing online pornography. Reducing minor access, even if not by 100%, advances the state's interest in protecting children from obscenity. Given the negligible cost of implementing the technology, age verification should be permissible under any level of scrutiny. *See* Texas Br. 32, 40–42.

Finally, parental controls, often touted as a less-restrictive alternative, impose more burdens on privacy than age verification.

ARGUMENT

I. Age-Verification Technologies Ensure Privacy at Low Cost

When the Court decided *Ashcroft*, the then-available age-verification technologies required users to provide sensitive personal information, such as government-issued identification or credit card details. In the two decades since, the technological landscape has evolved dramatically, making "reasonable age verification methods" far safer and less intrusive. Tex. Civ. Prac. & Rem. Code § 129B.002(a). Today, available technologies offer private and cost-effective methods to verify age. These advancements ensure that laws such as H.B. 1181 will impose negligible burdens on adult access to pornography.

A. Available Age-Verification Methods Protect Privacy and Cybersecurity

Age verification refers to a broad range of practices and technologies used to estimate or determine a user's age with varying degrees of certainty. Eric N. Holmes, Cong. Rsch. Serv., LSB11020, *Online Age Verification (Part I): Current Context* 2 (2023). Although older techniques used to verify age online often relied upon older technology, such as government-issued identification cards or credit cards, *see Ashcroft*, 542 U.S. at 662, contemporary and emerging technologies can largely mitigate privacy and data-security risks associated with older age-verification methods. In particular, ZKPs, biometric techniques, and trusted third-party verifiers can verify age with little or no risk to privacy.

1. Zero-Knowledge Proofs

ZKPs are cryptographic protocols that allow a user to prove they meet specific criteria—such as being over 18—without revealing any underlying personal information. As one expert explains:

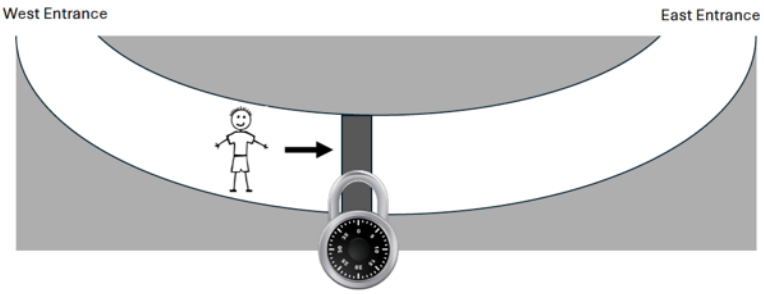
> With a zero-knowledge proof (ZKP), a party can prove that a statement is true without revealing any information except for whether it is indeed true or not. The obvious benefit is privacy since the prover does not need to reveal any additional information, and the second benefit is that it can significantly reduce the cost of verifying the correctness of a statement.

Alexander Berentsen et al., *An Introduction to Zero-Knowledge Proofs in Blockchains and Economics*, 105 Fed. Rsrv. Bank St. Louis Rev. 280, 280 (2023).

By providing only proof of a specific personal attribute, such as age, ZKPs are one of the most significant advancements in privacy-preserving identity management systems to date. *See* Jared Ronis, *Don't Trust When You Can Verify: A Primer on Zero-Knowledge Proofs*, Wilson Ctr. (Feb. 7, 2024), https://tinyurl.com/4rkfca7c. In fact, ZKPs are likely more private than presenting physical identification cards to brick-and-mortar retail stores. A physical identification card contains more information than what is necessary to verify whether a user exceeds a certain age (such as one's name, address, height, eye color, and even organ donor status), so the risk to privacy, while small, is greater. *Id.* Instead, because ZKPs allow for age verification without disclosing additional information, they offer not only superior privacy, but also

security against data breaches. *See id.* ("The adoption of ZKPs benefits individuals whose personal data remains protected and private as well as businesses, which can avoid the substantial financial and reputational damage often associated with such data breaches. By enhancing data security and integrity, ZKPs provide two key benefits: they help in building trust among consumers and simultaneously safeguard businesses against the risks and liabilities of data mismanagement.").

A metaphor known as "Ali Baba's Cave" can illustrate how ZKPs work. *See* Jean-Jacques Quisquater et al., *How to Explain Zero-Knowledge Protocols to Your Children*, 435 Lecture Notes in Comp. Sci. 628 (1989). Imagine a cave with two entrances, East and West. A door secured with a combination lock makes passing through the cave impossible. *See id.* at. 628–29. The Prover must demonstrate to the Verifier that the Prover knows the combination to the lock without disclosing the combination itself. By correctly and repeatedly appearing at different entrances based on the Verifier's instructions, the Prover demonstrates knowledge of the secret combination without revealing the combination (or any other information), as pictured in the following graphic. *Id.* at 630–31.



ZKPs often use a trusted third party to verify a user's eligibility—for example, a company that confirms the user's age through a government-issued identification, and then provides a unique cryptographic key to the user. *See, e.g.*, Adam Candeub, *Online Age-Verification: Protecting Children and Privacy*, Ctr. for Renewing Am. (July 21, 2023), https://tinyurl.com/5chhntjz. This key allows the user to prove age without transmitting any identifiable information. ZKPs are already widely used in cryptocurrency applications such as Zcash, demonstrating their scalability and security. Ronis, *supra* ("Several blockchain platforms have integrated ZKPs as a core component of their technology stack, fostering ready-built platforms for the development and deployment of ZKP-based applications.").

In 2022, researchers for France's data-protection agency developed a ZKP-based "age-verification system that allows accessing restricted websites without sharing other personally identifiable data." Jérôme Gorin et al., *Demonstration of a Privacy-Preserving Age Verification Process*, LINC (June 22, 2022), https://tinyurl.com/mr3epput. These systems are well-suited to verify age.

2. Biometric Age Verification and Estimation

Biometric systems offer another effective means to verify age online while protecting privacy. These systems use artificial intelligence ("AI") to analyze the

images, video, or voice recordings of a user, and verify or estimate a user's age.

Biometric methods can use low-resolution imagery to reduce privacy and cybersecurity risks. Low-resolution imagery ensures that fingerprints or facial scans cannot be extracted from the images, significantly mitigating privacy concerns. For example, artificial-intelligence systems can analyze facial features, walking gait, or other behaviors to determine age with remarkable accuracy. *See* Timilehin B. Aderinola et al., *Learning Age from Gait: A Survey*, 9 IEEE Access 100352, 100352 (2021).

When well designed, these systems effectively keep minors out, as they are difficult to evade and require no active monitoring from parents or guardians. For example, multimodal systems combine multiple biometric systems to add redundancies that substantially reduce the chance of evasion or false positives. *See, e.g.*, Vignesh Krisnakumar, *How Multimodal Biometrics Help with Age Verification and Compliance*, Biometric Update (Oct. 2, 2024), https://tinyurl.com/3zjpz3ax.

Yoti, an example Texas gives, *see* Texas Br. 9–10, includes a facial-age estimation technique that doesn't require an identification or credit card. *Age Check Users Globally from a Selfie*, Yoti, https://tinyurl.com/m2cfazy8 (last visited Nov. 20, 2024). Instead, it uses AI to confirm that the user's photo is of a real person and that the user is above a certain age. *See id.* The company tests the accuracy of its AI model to ensure that facial-age estimating is accurate across sexes and skin tones and unbiased. *Id.* In late October 2024,

Yoti's facial-estimating technology was re-evaluated by the U.K.'s Age Check Certification Scheme, an independent, government-accredited assessment body. Matt Prendergast, *Age Check Certification Scheme Evaluation for Yoti Facial Age Estimation*, Yoti Blog (Oct. 25, 2024), https://tinyurl.com/yumxafdd. The assessment found that "97.8% of 18 year olds are reliably estimated to be under 21," meaning "a very high percentage of adults can take a selfie and use Yoti [facial-age estimating] to show they are 18 or over." *Id.* Yoti works well.

3. Trusted Third-Party Verifiers

Yet another alternative is to use a trusted third-party verifier. For example, Louisiana's LA Wallet allows users to keep a digital representation of a driver's license on mobile devices, offering seamless, privacy-preserving age verification for smartphone users and businesses. *See Bring Digital Verification to Your Business*, LA Wallet, https://tinyurl.com/yu6tk9s5 (last visited Nov. 17, 2024). No copy of the physical identification is stored in LA Wallet's servers. *Digital Capabilities for Real Time Identification*, LA Wallet, https://tinyurl.com/mvz9f4rj (last visited Nov. 17, 2024).

Louisiana, like Texas, has also enacted an age-verification law to restrict minors' access to harmful online content. *See* La. Stat. Ann. § 9:2800.29. LA Wallet provides one method of age verification. When the application communicates with a website requesting age verification, it confirms only that the user meets the age requirement. No other personal information is transmitted, stored, or retained when verifying age.

Id. § 9:2800.29(B)(2) ("Any commercial entity or third party that performs the required age verification shall not retain any identifying information of the individual after access has been granted to the material.").

LA Wallet's age-verification process is simple and efficient:

1. The user selects "Verify with LA Wallet" on the requesting website.
2. The website generates a unique "Verify You" code, which the user inputs into the LA Wallet application.
3. The application confirms whether the user is over 18, without revealing other information.
4. The user then selects "Approve" to complete the remote age verification.

Cf. Using Remote Verify You / Verification, LA Wallet (Oct. 9, 2024), https://tinyurl.com/4vztd4bs. This process takes less than 45 seconds and effectively deters minors, as minors cannot easily falsify or obtain digital identifications. The system has been widely adopted in Louisiana and serves as a model for other jurisdictions.

Other states, including Arizona and California, have implemented similar third-party systems, showing these systems are scalable and versatile. For example, as part of California's pilot program for digital driver's licenses, the California Department of Motor Vehicles recently held a "hackathon"—an event that brings together computer engineers to collaborate on a new software solution. *See, e.g.*, Lauren Martinez, *Digital ID: Here's How Mobile Driver's License Tech Could*

Be Used by Bay Area Businesses, ABC 7 News (Oct. 2, 2024), https://tinyurl.com/3w68su2v; *Hackathon*, Meriam-Webster Online Dictionary, https://tinyurl.com/bdhwapaz (last visited Nov. 21, 2024). The Department gave the "Best Privacy & Security Design" award to an engineering team from the financial technology firm Block, which offers the popular Square point-of-sale payment system. Angie Jones, *Our California DMV Hackathon Win: Privacy-Preserving Age Verification* (Oct. 15, 2024), https://tinyurl.com/ys9unyjd. Block's team developed an instant age-verification system using California's mobile driver's licenses "to provide secure, privacy-centric transactions for age-restricted purchases with Square's Point of Sale (POS) system." *Id.* As Block explains, by "focusing solely on verifying the specific data point needed (in this case, whether someone is over 21), we avoid collecting or storing any unnecessary information. This is a win for both businesses and consumers, as it minimizes risk while maintaining a smooth user experience." *Id.*

Apart from digital identification technologies, private third-party firms such as Yoti offer easy, quick, and privacy-protecting tools to estimate and verify age. Users can verify their age through various methods, including uploading government-issued identification, inputting their cellular-provider information, or taking a "selfie" with their smartphone's front-facing camera. *Age Verification*, Yoti, https://tinyurl.com/46mejx6d (last visited Nov. 20, 2024). Regardless, Yoti's tools "let users prove they're the right age for [an age-restricted] service without sharing any personal information," and Yoti doesn't "share or store any personal data." *Id.*

Users don't need to verify their age each time they visit a website. Yoti gives age-verified users a reusable digital token, which provides proof of age for later visits to the same website. *See Reusable Age Checks*, Yoti, https://tinyurl.com/3frn4n4n (last visited Nov. 21, 2024). If other websites accept Yoti's token, then users need not validate their age again on those websites. *Age Verification*, Yoti, *supra*. Tokens protect user privacy, as they "don't contain any personal details, just the result of an age check and information around when and how it was performed." *Id.*

Well-known technology firms use Yoti's technology. Meta, the parent company of Facebook and Instagram, uses Yoti to verify that "Facebook Dating" users are at least 18 years old. Erica Finkle, *Bringing Age Verification to Facebook Dating*, Meta Newsroom (Dec. 5, 2022), https://tinyurl.com/axwf9sc7. As Meta's director of data governance explained, "Yoti's technology estimates your age based on your facial features, shares that estimate with us and the image is then deleted immediately. The technology cannot recognize your identity— just your age." *Id.*

B. Age Verification Is Inexpensive

Modern age-verification systems eliminate the cost and inconvenience associated with the outdated methods identified in *Ashcroft*. *See Ashcroft*, 542 U.S. at 682 (Breyer, J., dissenting) (noting the then estimated cost to store credit-card numbers or passwords at 15 to 20 cents per number, and less than $20 per year for users).

Digital identification systems such as LA Wallet are free and require no additional hardware or complex setups. For example, Arizona's Smart ID Verifier application allows businesses to confirm a customer's age using digital identifications stored in Apple Wallet or Google Wallet. *See Smart ID Verifier App*, Arizona Dep't of Transp., https://tinyurl.com/bdebj9uu (last visited Nov. 17, 2024). The application verifies age without sending unnecessary data, ensuring privacy at low cost for users and businesses. Arizona Dep't of Transp., Press Release, *Adot Mvd Offers Retailers a New App for Mobile ID Age Verification* (July 30, 2024), https://tinyurl.com/323bj6kh ("Retailers using the Smart ID Verifier app will only be provided the required information necessary for age verification, such as a customer's age and ID photo.").

Similarly, commercial solutions such as Microsoft Entra Verified ID and Mastercard ID offer scalable and cost-effective verification tools that integrate seamlessly into existing digital systems. *See, e.g.*, Microsoft Security, *Microsoft Entra Verified ID* 1 (2004), https://tinyurl.com/2s43b4an. These solutions include privacy protections as an inherent feature. *Id.* (assuring business clients and their users that their data privacy is protected through "proactively transparent, privacy-respecting, and minimally invasive identity checks").

Age verification does not have to be the hassle that some critics, including Petitioners, make it out be. Modern technology allows for seamless, privacy-preserving solutions built into device-operating systems and browsers. As mentioned, services such as Yoti allow users to verify their age once and receive a secure

digital token that can be reused across devices and participating websites. When visiting the new site, the system simply checks for a valid age token—if present, users can enter immediately without re-verifying. If not, then they can complete a one-time verification to receive a token for future use. These tokens can be configured with different duration periods and verification methods, while maintaining privacy by only sharing a user's age. When users visit age-restricted services, their device can simply send a signal confirming their adult status. *See Reusable Age Checks*, Yoti, *supra*. Age verification could also occur during set up on phones, tablets, and browsers similar to the way users set up "Face ID" on an iPhone for quick and painless access. This streamlined approach protects both privacy and convenience.

II. Governments Often Require Age Verification

In recent years, U.S. states and foreign countries have required websites to verify age for a wide variety of purposes. Governments already require age verification for adult activities ranging from online sports betting to online banking. For example, the fantasy sports betting platform DraftKings uses age verification to comply with laws governing access to online gaming activities. *See* DraftKings Inc., Registration Statement (Form S-1), at 78 (May 6, 2020), https://tinyurl.com/52nsc364 ("[W]e employ various methods and tools across our operations such as … age verification to ensure our users are old enough to participate.").

The rapid growth in online banking has also prompted the development of age-verification methods upon opening an account, sometimes through third-party providers. *See How Do You Check Age Online?*, Age Verification Providers Ass'n, https://tinyurl.com/yenspua5 (last visited Nov. 17, 2024) ("Some banks allow trusted third parties to confirm a date of birth supplied to by the customer with those records. Typically, the user logs into their own online banking system, and gives approval for the data to be supplied to the third party, which in this case would be an age verification provider."). The ubiquity of online banking and other applications where age verification is necessary suggests that private actors—including operators of adult websites—can readily adapt to HB 1181's requirements.

Many countries—including the United Kingdom, Germany, and France—require adult websites to verify their users' age. *See, e.g.*, Manuel G. Pascual, *How Age Verification to Access Porn Works in France: 'They Won't Know Anything About You, Other Than That You're an Adult,'* El Pais English (May 7, 2024), https://tinyurl.com/4v45erjb.

In December 2023, the European Union required the world's three largest adult websites to verify their users' ages. Kelvin Chan, *Three of the Biggest Porn Sites Must Verify Ages to Protect Kids Under Europe's New Digital Law*, AP (Dec. 20, 2023), https://tinyurl.com/3m2wemcr.

Many firms, especially ones with substantial online traffic, comply with more stringent privacy regulations than required under U.S. law, including the

European Union's General Data Protection Regulation. *See* Kevin E. Davis & Florencia Marotta-Wurgler, *Filling the Void: How E.U. Privacy Law Spills Over to the U.S.*, J.L. & Empirical Analysis 1, 1 (2024) ("In fact, 75% of the firms in our sample use the same privacy policy for their U.S. and E.U.-facing websites."). These regimes lower the risk of data breaches or misuse.

III. Online Activity Isn't Private Anyway

In *Ashcroft*, the Court assumed that age-verification systems would transform an otherwise anonymous online experience into one where a user's identity is publicly exposed, leading to embarrassment and potential chilling effects on adult access to constitutionally protected content. *See Ashcroft*, 542 U.S. at 667. That is no longer true. Online activities today are already extensively tracked and recorded, often without the user's knowledge or consent. Age-verification systems using contemporary privacy-preserving technologies don't meaningfully increase these privacy risks.

Most websites and online services use tracking technologies such as cookies and device fingerprinting. *How Websites and Apps Collect and Use Your Information*, U.S. Fed. Trade Comm'n (Sept. 2023), https://tinyurl.com/bsvxv3c8. These tools create detailed user profiles by analyzing browsing history, device characteristics, and geolocation data. *Id.* For example, cookies allow websites to track users' behavior over time, enabling targeted advertising and personalized content but also compromising anonymity. *See id.*

Even when users are not logged into accounts, digital fingerprints—unique combinations of device settings, screen resolutions, and browser plugins—allow companies to identify and track them. *See Browser Fingerprinting—A Thorough Overview*, fraud.com, https://tinyurl.com/2vy8aeus (last visited Nov. 21, 2024). These profiles are frequently monetized by data brokers and are often traceable to particular users with minimal effort. Internet service providers ("ISPs") and device manufacturers can readily associate IP addresses with specific users or households, and do so readily when compelled by law-enforcement subpoenas.

In today's heavily tracked internet, *Ashcroft*'s romantic notion of online anonymity is illusory. Age-verification systems leveraging privacy-preserving methods, such as ZKPs or trusted third-party verifiers, don't expose users to greater privacy risks than they face already by browsing. Instead, these systems allow users to verify their eligibility for restricted content without disclosing sensitive information or creating additional tracking points.

As a practical matter, users seeking access to adult content are already navigating a system that compromises privacy. Search engines, social-media platforms, and adult content websites routinely collect vast amounts of data on their users, including browsing and purchasing habits. In many cases, this data is stored indefinitely and shared across platforms for marketing. Age-verification systems that limit data collection to a single verification point, without retaining or transmitting personal information, improve privacy.

Today's quite public online reality suggests that online businesses shouldn't be more protected than brick-and-mortar stores. In *Ginsberg v. New York*, this Court upheld a New York law requiring in-person age verification for the purchase of sexually explicit materials. The Court recognized that even face-to-face verification, which involves direct interaction and potential embarrassment, was a permissible burden on speech when balanced against the state's interest in protecting minors. *See* 390 U.S. at 638. Digital age-verification systems impose fewer burdens while achieving the same objectives.

Unlike the in-person verification requirement upheld in *Ginsberg*, modern age-verification technologies operate invisibly, without requiring users to interact with another person or publicly disclose their age. *See* Ronis, *supra*. Systems such as Louisiana's LA Wallet, California's DMV Wallet, or biometric age estimators allow users to verify their age anonymously and in seconds. *See, e.g.*, AuthenticID, Press Release, *California DMV Fortifies Mobile Driver's License (mDL) Enrollment with AuthenticID's Identity Verification Technology*, (Nov. 13, 2024), https://tinyurl.com/mry53c9k. These systems eliminate the stigma associated with in-person checks by ensuring that verifying parties don't retain a user's personal identifying information, let alone share it. *See, e.g.*, La. Stat. Ann. § 9:2800.29(B)(2).

The Court shouldn't treat brick-and-mortar stores worse than online businesses. That would create an uneven playing field in the market for content. *Cf. South Dakota v. Wayfair*, 585 U.S. 162, 179 (2018). If in-person verification laws at brick-and-mortar stores

are constitutional, then it is unclear why digital age-verification laws, which are less invasive, wouldn't be equally permissible for businesses that move their content online. By verifying age without requiring users to disclose their identity to a third party, these laws protect minors while burdening adult access to online content less than in-person verification requirements. *See* Ronis, *supra*.

IV. Age Verification Helps Even if Some Minors Evade It

Petitioners and other critics of age verification argue that minors can evade age-verification systems using Virtual Private Networks ("VPNs") or shared credentials. *See* Texas Br. 40–41 (discussing and responding to these arguments); *see also* Lauren Leffer, *Online Age Verification Laws Could Do More Harm Than Good*, Sci. Am. (Apr. 16, 2024), https://tinyurl.com/3sy2d4r4.

Although no system is foolproof, modern age-verification technologies would prevent more minors from accessing obscene content. Age-verification technologies such as LA Wallet, AI-driven biometrics, and hard-to-falsify digital identifications, significantly reduce minors' access to harmful content compared to the status quo. Although some motivated and crafty minors may find ways to bypass these systems, age verification erects a meaningful barrier that will likely prevent most minors from accessing unauthorized content. Texas Br. 41.

Age verification is difficult for minors to evade. For example, users ordinarily obtain VPN access as a

paid service, usually requiring a credit or debit card payment. As minors are generally prohibited from having a credit card or bank account (in their own names), *see, e.g.*, Credit Card Accountability Responsibility and Disclosure Act of 2009, Pub. L. No. 111-24, § 301, 123 Stat. 1734, 1748, *codified at* 15 U.S.C. § 1637(c)(8), they have to use adult credit cards or bank accounts, which would generate transaction notifications visible to parents. This oversight has a deterrent effect, limiting minors' ability to use tools for evasion without parental detection.

Digital-identification systems, such as LA Wallet, rely upon secure encryption and trusted issuing authorities, making them more resistant to forgery than traditional forms of identification. *See, e.g.*, Ash Johnson, *The Path to Digital Identity in the United States* 3 (2024), https://tinyurl.com/3zxu2xum ("The transition from physical wallets to mobile wallets also brings with it increased security. … If designed correctly, digital ID can also be more privacy-protective than physical ID.") These identifications are tied to verified credentials, ensuring that minors cannot easily impersonate adults. *See id.*

Biometric systems analyze unique adult behavioral traits that are difficult to replicate, such as arm movements or gait. *See* Aderinola, *supra*, at 100357–58. These systems provide an added layer of security, reducing the likelihood of evasion even if minors gain access to adult credentials.

V. Parental Controls Are More Invasive than Age Verification

Parental controls such as content filtering, a commonly touted "less restrictive" alternative to age verification, are particularly invasive. Parental controls rely upon a third-party company to collect and monitor a minor's activities and communications. These controls often require parents to grant access privileges to technology companies. For example, over 80% of parental-control applications on Google Play Store request access to location, contacts, and storage, and 72% shared data with third parties without notifying users in their privacy policy. Álvaro Feal et al., *Angel or Devil? A Privacy Study of Mobile Parental Control Apps*, 2 Proc. Priv. Enhancing Tech., 314, 314, 320 (2020), https://tinyurl.com/yck4rbty. Nearly three-quarters of parental-control applications incorporate "libraries" that collect and share data through advertising networks, social media platforms, and analytics services. *Id.* at 315.

Parental-control applications are also vulnerable to device compromise, account takeover, data leakage, and insecure transmission of personally identifiable information. *See* Suzan Ali et al., *Betrayed by the Guardian: Security and Privacy Risks of Parental Control Solutions*, *in* Procs. of the 36th Ann. Computer Sec. Applications Conf. 69, 79–80 (2020). For example:

- In 2019, Apple removed a number of parental control applications from its App Store because "they put users' privacy and security at risk," explaining that several were using highly invasive tactics that give third-party control and ac-

cess over devices, as well as sensitive data including location, camera permissions, and browsing history. Apple, Media Statement, *The Facts About Parental Control Apps* (Apr. 28, 2019), https://tinyurl.com/2a4563a5.

- In 2018, Family Orbit, which markets itself as "the best parental control app to protect your kids," exposed 281 gigabytes of monitored children's photos online. Lorenzo Franceschi-Bicchierai, *Spyware Company Exposed '281 Gigabytes' of Children's Photos Online*, Vice (Apr. 30, 2018), https://tinyurl.com/ycy7nmm3.
- In another breach that year, TeenSafe, which allows parents to view text, call logs, web history, installed apps, and location on phones, leaked thousands of email addresses and plaintext passwords. Zack Whittaker, *Teen Phone Monitoring App Leaked Thousands of User Passwords*, ZDNet (May 20, 2018), https://tinyurl.com/yc7828ny/.

Children's data are actually more valuable and more vulnerable to abuse. Kavitha Cardoza, *Hackers are Targeting a Surprising Group of People: Young Public School Students*, NPR (Mar. 12, 2024), https://tinyurl.com/32eytcvw. Not only are these technologies usually less effective at preventing minor access to obscene content: they also impose a greater burden on internet users' online privacy.

CONCLUSION

Modern technologies have resolved longstanding criticisms of age verification, effectively advancing the state's interest in protecting minors from harmful online content while minimally burdening adult access to protected content. These systems employ robust privacy-preserving mechanisms, design features, and enforcement measures that minimize the incidental burden on adult speech. Accordingly, under any level of scrutiny, the Court should affirm the Fifth Circuit's judgment.

Respectfully submitted,

ILYA SHAPIRO
JOHN KETCHAM
TIM ROSENBERGER
MANHATTAN INSTITUTE
52 Vanderbilt Ave.
New York, NY 10017
(212) 599-7000
ishapiro@manhattan.institute

JONATHAN BERRY
JAMES R. CONDE
Counsel of Record
ADAM H CHAN
BOYDEN GRAY PLLC
800 Connecticut Ave. NW,
Suite 900
(202) 955-0620
jconde@boydengray.com

November 22, 2024