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 *AMICI CURIAE* THE CENTER FOR DEMOCRACY & TECHNOLOGY, NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE, THE INTERNET SOCIETY, PROFESSOR DANIEL WEITZNER, PROFESSOR ERAN TROMER, AND PROFESSOR SARAH SCHEFFLER IN SUPPORT OF PETITIONERS

ANDREW S. BRUNS
Counsel of Record
AMOS J. B. ESPELAND
COURTNEY J. LISS
IMARA MCMILLAN
KEKER, VAN NEST & PETERS, LLP
633 Battery Street
San Francisco, CA 94111
(415) 391-5400
abruns@keker.com

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF CONTENTS i

TABLE OF CITED AUTHORITIES iv

INTRODUCTION AND INTEREST OF *AMICI CURIAE* 1

SUMMARY OF ARGUMENT 3

ARGUMENT 4

I. Five Existing Age Verification Methods Conceivably Satisfy Texas HB 1181 4

II. Existing Age Verification Technologies Are Often Ineffective and Present Privacy and Security Risks 7

A. Uploading a Government-Issued ID 7

1. Effectiveness 9

2. Security and Privacy Risks 13

B. Authorizing Temporary Credit or Debit Card Charges 15

1. Effectiveness 16

2. Security and Privacy Risks 17

C. Third-party Databases and Analysis 19

1. Effectiveness 19

2. Security and Privacy Risks 20

D. Biometric Scanning 21

1. Effectiveness 22

2. Security and Privacy Risks 26

E. First-party Signal Analysis 27

1. Effectiveness 28

2. Security and Privacy Risks 29

III. The Ineffectiveness of Current Age Verification Methods, Combined with the Technologies' Security and Privacy Risks, Unconstitutionally Burden Adults' Access to Constitutionally Protected Speech and Render HB 1181 Both Under and Overinclusive 30

A. Implementing HB 1181 With Current Technology Will Necessarily Prevent Some Adults from Accessing Some Protected Content Altogether 30

B. The Security and Privacy Risks Associated with Current Technologies–Including That Sensitive Browsing Activity Will Be Deanonymized–Also Burdens Adults' Access to Protected Content ...31

C. HB 1181 Will Also Fail to Achieve its Purpose of Protecting Children Because They Can Easily Circumvent Current Age Verification Technologies 35

D. HB 1181's Non-retention Requirement Is Insufficient to Address These Risks.....36

CONCLUSION 38

TABLE OF AUTHORITIES

Cases

Ashcroft v. ACLU, 542 U.S. 656 (2004) 1, 29

Ginsberg v. New York, 390 U.S. 629 (1968) 3

Reno v. ACLU, 521 U.S. 844 (1997).....29

Statutes and Other Authorities

15 U.S.C. §§ 1601-1667f.....16

AG Healey Secures $16 Million from Multistate Settlements with Experian and T-Mobile Over Data Breaches, Mass. Office of the Att'y Gen. Press Release (Nov. 7, 2022), https://www.mass.gov/news/ag-healey-secures-16-million-from-multistate-settlements-with-experian-and-t-mobile-over-data-breaches 32

Att'y Gen. of Tex., *Data Security Breach Reports*, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited Sept. 17, 2024).....37

Biometric Data, ID4D Practitioner's Guide: Version 1.0, World Bank (October 2019), https://id4d.worldbank.org/guide/biometric-data.....27

Jennifer Bryant, *The 'growing ecosystem' of age verification,* Intl. Assoc. of Privacy Pro. (Mar. 28, 2023), https://iapp.org/news/a/the-growing-ecosystem-of-age-verification 21

Daniel Castro, Information Technology & Innovation Foundation, *Protecting Children Online Does Not Require ID Checks for Everyone* (November 21, 2023), https://itif.org/publications/2023/11/21/protecting-children-online-does-not-require-id-checks-for-everyone/ 9, 11

Clare Y. Cho, Cong. Rsch. Serv., R47884, *Identifying Minors Online* (Jan. 2, 2024), https://crsreports.congress.gov/product/pdf/R/R47884 34

Cristina Criddle, *Web browsing data collected in more detail than previously known, report finds*, Financial Times (Nov. 13, 2023), https://www.ft.com/content/6c8f1f24-b690-4bbd-b726-28b2d6f10800 33

Declaration of Richard I. Sonnier III in Support of Plaintiffs' Motion for Expedited Preliminary Injunction, *Free Speech Coalition, Inc. v. Paxton*, No. 1:23-cv-00917-DAE (W.D. Tex. August 4, 2023), ECF No. 5-2 ("Sonnier Decl.") 9

Pavni Diwanji, *How Do We Know When Someone Is Old Enough to Use Our Apps?,* Meta Newsroom (Jul. 27, 2021); https://about.fb.com/news/2021/07/age-verification/.....28

Equifax, *Age Verification,* https://www.equifax.co.uk/business/age-verification/en_gb/ (last visited Sep. 17, 2024).....32

Experian, *Age verification services for your business*, https://www.experian.co.uk/business/regulation-and-fraud/identity-checks/age-verification (last visited Sep. 17, 2024) 32

F.D.I.C., *2021 FDIC National Survey of Unbanked and Underbanked Households, 2021 Executive Summary*, (Oct. 2022).....17

F.T.C., *Equifax Data Breach Settlement*, F.T.C. (Feb. 2024), https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement 32

Erica Finkle et al., *How Meta uses AI to better understand people's ages on our platforms* (June 22, 2022), https://tech.facebook.com/artificial-intelligence/2022/06/adult-classifier/ 7, 28

Sarah Forland, Nat Meysenburg & Erika Solis, *Age Verification: The Complicated Effort to Protect Youth Online*, New America 20 (Apr. 23, 2024), https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/challenges-with-age-verification/ 6, 10

FTC Warns About Misuses of Biometric Information and Harm to Consumers, F.T.C. Press Release (May 18, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers.....26

Samuel Gibbs, *Adult Friend Finder and Penthouse hacked in massive personal data breach,* The Guardian (Nov. 14, 2016), https://www.theguardian.com/technology/2016/nov/14/adult-friend-finder-and-penthouse-hacked-in-largest-personal-data-breach-on-record 34

Andy Greenberg, *OPM Now Admits 5.6m Feds' Fingerprints Were Stolen By Hackers*, Wired (Sep. 23, 2015, 11:30 AM), https://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers/ 26

Jonathan Greig, *More than 400,000 have data leaked in cyberattack on Texas education organization*, The Record (June 20, 2024), https://therecord.media/texas-atpe-educators-data-breach-notification 37

Michael J. Hammer & Samuel B. Novey, *Who Lacked Photo ID in 2020?* 2-3, Center for Democracy and Civil Engagement (Mar. 13, 2023), https://www.voteriders.org/wp-content/uploads/2023/04/CDCE_VoteRiders_ANES2020Report_Spring2023.pdf.....11, 12

Kayee Hanaoka et al., *Face Analysis Technology Evaluation: Age Estimation and Verification*, National Institute of Standards and Technology, U.S. Dept. of Commerce (May 2024), https://doi.org/10.6028/NIST.IR.8525 .....23, 31

Bethany Hickey, *Best credit cards for teens under 18,* Finder (Sept. 4, 2024), https://www.finder.com/kids-banking/credit-card-options-teens 16

Chelsea Jarvie and Karen Renaud, *Are you over 18? A Snapshot of Current Age Verification Mechanisms* 12, Proceedings of 2021 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop (2021), https://strathprints.strath.ac.uk/82540/ 26

Ali Juell, *New Study: Texas' undocumented immigrant population remained relatively stable in 2021*, The Tex. Trib. (Nov. 21, 2023), https://www.texastribune.org/2023/11/21/texas-immigrants-pew-research/ 12

Jason Kelley, *Hack of Age Verification Company Shows Privacy Danger of Social Media Laws,* Electronic Frontier Foundation (June 26, 2024), https://www.eff.org/deeplinks/2024/06/hack-age-verification-company-shows-privacy-danger-social-media-laws.....32

Youssef A. Kishk*, State-Based Online Restrictions: Age-Verification And The VPN Obstacle In The Law*," 2 Int'l J. L. Ethics Technology 150 (2024), https://www.doi.org/10.55574/VBDM8223 9

Pavel Korshunov et al., *Vulnerability of Face Age Verification to Replay Attacks* 1-2, IEEE International Conference on Acoustics, Speech, and Signal Processing (2014), https://publications.idiap.ch/attachments/papers/2024/Korshunov_ICASSP_2014.pdf 25

Stuart Madnick, *Why Data Breaches Spiked in 2023*, Harvard Bus. Rev. (Feb. 19, 2024), https://hbr.org/2024/02/why-data-breaches-spiked-in-2023 20

Marley Malenfant, *What is the SCOPE Act? New Texas law requires parental approval over kids' social media,* Austin American-Statesman (Sept. 13 .2024), https://www.statesman.com/story/news/state/2024/09/13/scope-act-texas-hb-18-social-media-children-personal-data-online-judge-robert-pitman-block/75178891007/ 30

Toni Matthews-El et al., *Is Using a VPN Safe? What You Need To Know About VPN Security,* Forbes Advisor (June 1, 2024), https://www.forbes.com/advisor/business/software/are-vpns-safe/ 35

Rachel Metz, *A reporter tried the AI Instagram wants to use to verify age. Here's what it found,* CNN Business (June 27, 2022, 7:30 PM), https://www.cnn.com/2022/06/27/tech/instagram-ai-age-estimation-face-scan/index.html 21

H. Otto et al., *Age estimation from face Images: Human vs. machine performance*, IEEE IAPR Int'l Conference on Biometrics, Madrid, Spain (June 4-7, 2013), https://doi.org/10.1109/ICB.2013.6613022) 22

Overview of Members' services, The Age Verification Providers Association, https://avpassociation.com/find-an-av-provider/ (last visited Sept. 17, 2024) 4

Jule Pattinson-Gordon, *Report: Biometric Injection Attacks on the Rise,* Government Technology (Mar. 15, 2024), https://www.govtech.com/security/report-biometric-injection-attacks-on-the-rise 35

Toni Perkins-Southam & Caroline Lupini, *Can I Add My Child To My Credit Card?*, Forbes Advisor (Jan. 11, 2024, 4:59 PM), https://www.forbes.com/advisor/credit-cards/should-you-add-your-children-as-authorized-user-on-your-credit-card/.....16

Public Interest Research Group, *How Mastercard sells its 'gold mine' of transaction data*, (Updated June 17, 2024), https://pirg.org/edfund/resources/how-mastercard-sells-data/.....18

Jillian Andres Rothschild, Samuel B. Novey & Michael J. Hammer, *Who Lacks ID in America Today?" An Exploration of Voter ID Access, Barriers, and Knowledge*, Center for Democracy and Civic Engagement (Jan. 2024), https://cdce.umd.edu/sites/cdce.umd.edu/files/pubs/Voter%20ID%202023%20survey%20Key%20Results%20Jan%202024%20%281%29.pdf.....12

Sarah Scheffler, *Age Verification Systems Will Be a Personal Identifiable Information Nightmare,* Communications of the ACM (June 10, 2024), https://cacm.acm.org/opinion/age-verification-systems-will-be-a-personal-identifiable-information-nightmare/#B1 39

Lauren Silverman, *Turning to VPNs for Online Privacy? You Might Be Putting Your Data At Risk,* NPR (Aug. 17, 2017), https://www.npr.org/sections/alltechconsidered/2017/08/17/543716811/turning-to-vpns-for-online-privacy-you-might-be-putting-your-data-at-risk 35

Bridget Small, F.T.C, *Consumer Alert: Scam emails demand Bitcoin, threaten blackmail,* FTC Consumer Advice (Apr. 29, 2020), https://consumer.ftc.gov/consumer-alerts/2020/04/scam-emails-demand-bitcoin-threaten-blackmail 34

Michael Smith et al., *Browser history re:visited*, 12th USENIX Workshop on Offensive Technologies (2018), https://www.usenix.org/conference/woot18/presentation/smith 13

Jackie Snow, *Why Age Verification Is So Difficult for Websites*, Wall Street J. (Feb. 27, 2022, 8:00 am ET), https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728?st=f0lp8y2cgptjoyb&reflink=article_email_share 16, 17

Zahra Stardust et al., *Mandatory age verification for pornography access: Why it can't and won't 'save the children,'* Big Data & Soc'y 5 (2024), https://journals.sagepub.com/doi/pdf/10.1177/20539517241252129.....22, 24

Tex. Att'y Gen., *Texas Data Privacy and Security Act,* https://www.texasattorneygeneral.gov/consumer-protection/file-consumer-complaint/consumer-privacy-rights/texas-data-privacy-and-security-act, (last visited Sept. 17, 2024).....14

Tex. H.B. 71, 88th Leg., Reg. Sess. (2023), https://capitol.texas.gov/BillLookup/History.aspx?LegSess=88R&Bill=HB71 5

Using technology to more consistently apply age restrictions, YouTube Official Blog (Sept. 22, 2020), https://blog.youtube/news-and-events/using-technology-more-consistently-apply-age-restrictions/.....15

Ramon Antonio Vargas, *Every Louisiana driver's license holder exposed in colossal cyber-attack,* The Guardian (June 16, 2023, 12:21 EDT), https://www.theguardian.com/us-news/2023/jun/16/louisiana-drivers-license-hack-cyber-attack 13

Veriff, *Age Validation*, https://www.veriff.com/product/age-validation (last visited Sept. 19, 2014).....8, 11

Daniel Victor, *The Ashley Madison Data Dump, Explained*, N.Y. Times (Aug. 19, 2015), https://www.nytimes.com/2015/08/20/technology/the-ashley-madison-data-dump-explained.html.....34

Shoshana Weissman & Canyon Brimhall, *Age-verification laws don't exempt VPN traffic. But that traffic can't always be detected*, R Street Institute (Aug. 29, 2023), https://www.rstreet.org/commentary/age-verification-laws-dont-exempt-vpn-traffic-but-that-traffic-cant-always-be-detected/ 35

White House, *FACT SHEET: President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data* (Feb. 28, 2024), https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/ 34

Yoti, *Yoti Facial Age Estimation* (Dec. 2023), https://www.yoti.com/wp-content/uploads/2024/04/Yoti-Age-Estimation-White-Paper-December-2023.pdf.....25

INTRODUCTION AND INTEREST OF *AMICI CURIAE*[1]

"A serious flaw in any case involving the Internet" is that the "factual record does not reflect current technological reality[.]" *Ashcroft v. ACLU,* 542 U.S. 656, 671 (2004). As the Court considers the level of scrutiny to apply to laws requiring adults and children alike to verify their age to access certain websites, *Amici* nonprofit technology organizations and professors seek to provide the Court with information demonstrating that the current technological reality of implementing such legislation means that it will burden adults' access to constitutionally protected speech.

The Center for Democracy and Technology (CDT) is a non-profit, public interest organization that for over 25 years has worked to promote the constitutional and democratic values of free expression, privacy, equality, and individual liberty in the digital age.

New America's Open Technology Institute (OTI) is a non-profit organization working to ensure that every community has equitable access to technology

---

[1] *Amici* certify that no counsel for a party authored this brief in whole or in part, and no such counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No persons other than the *amici* or their counsel made any monetary contribution to this brief's preparation or submission.

and its benefits. OTI works to ensure that technological design, use, and governance promote security, safeguard rights, and further economic and political well-being.

The Internet Society is a global charity and nonprofit organization with the vision that the Internet is for everyone. Its primary objective is to coordinate and collaborate on issues related to improving the Internet, including standards, applications, and policies, and defend against actions that threaten the way that the Internet operates.

Profs. Daniel Weitzner, Eran Tromer, and Sarah Scheffler are researchers who together have written over 100 research papers for top security, privacy, and cryptography conferences.

Daniel J. Weitzner is a 3Com Founders Senior Research Scientist at the MIT Computer Science and Artificial Intelligence Lab and Founding Director of the MIT Internet Policy Research Initiative. His research focuses on privacy, cybersecurity and policies that enable the free flow of information online. From 2011-12, Weitzner was the White House Deputy Chief Technology Officer for Internet Policy.

Eran Tromer is a Professor of Computer Science at Boston University who has researched cybersecurity risks, deanonymization of personal information, and privacy-preserving regulatory compliance.

Sarah Scheffler is an Assistant Professor at Carnegie Mellon University who researches private

verifiable content moderation systems and contributed public and private comments to policymakers for the UK's Safety Tech Challenge regarding its Online Safety Act.

SUMMARY OF ARGUMENT

Texas House Bill 1181 requires websites containing a certain amount of content deemed "sexual material harmful to minors" to verify the age of visitors before granting access. But while advocates for the law argue this requirement is merely the digital equivalent of the ban on knowing sales to minors validated by this Court in *Ginsberg v. New York*, the limitations of current age verification technology—and the difference between the internet's inherent capability to transmit and make available uploaded identifying data and the ability of a stationery-store owner to recall such data from a quick flash of ID—create a significantly higher burden on adult access to protected content. 390 U.S. 629 (1968).

First, Amici describe how current technological methods available to satisfy HB 1181's age verification requirements are ineffective and pose security and privacy risks to individuals.

Second, Amici explain how, as a result of these limitations, requiring the use of these technologies will significantly burden adults' access to protected content.

ARGUMENT

I. Five Existing Age Verification Methods Conceivably Satisfy Texas HB 1181.

Texas House Bill 1181, codified at Tex. Civ. Prac. & Rem. Code Ann. § 129B.001 et seq. ("HB 1181"), requires that "[a] commercial entity that knowingly and intentionally publishes or distributes material on an Internet website . . . more than one-third of which is sexual material harmful to minors, shall use reasonable age verification methods . . . to verify that an individual attempting to access the material is 18 years of age or older." Section 129B.002(a). In other words, certain website operators must verify the ages of visitors before granting the visitors access to their websites.

HB 1181 demands that the "commercial entity" that publishes websites subject to the law or "a third party"[2] "shall" perform age verification by "requir[ing]" individuals attempting to access the website to (1) "provide digital identification," or (2) "comply with a commercial age verification system that verifies age using" (A) "government-issued identification"; or (B) "a commercially reasonable method that relies on public or private transactional data to verify the age of an individual." Section 129B.003(b).

---

[2] Most websites rely on third-party commercial vendors to perform age-verification checks, adding an additional layer of data privacy risk to such verifications. *See Overview of Members' services,* The Age Verification Providers Association, https://avpassociation.com/find-an-av-provider/ (last visited Sept. 17, 2024).

The first statutory category, age verification by "digital identification" under Section 129B.003(b)(1), is not currently possible in Texas. In 2023, the Texas House of Representatives passed HB 71, which would have required the Department of Public Safety to "establish a program for the issuance of digital identification." Tex. H.B. 71, 88th Leg., Reg. Sess. § 526.0102(a), (2023). The Senate took up the bill and referred it to the Committee on Transportation, where it has remained since May of last year.[3] As a result, Texans cannot provide a Texas-issued "digital identification."

The second statutory category permits age verification by a "commercial age verification system" using "government-issued identification[.]" Section 129B.003(b)(2)(A). This method requires Texans to upload a copy of their government-issued identification documents ("IDs"), such as a drivers' license, to the website or third-party verifier.

The third and broadest statutory category permits age verification by compliance with "a commercially reasonable age verification method that relies on public or private transactional data to verify the age of the individual." Section 129B.003(b)(2)(B). "Transactional data" is defined as "a sequence of information that documents an exchange, agreement, or transfer between an individual, commercial entity,

---

[3] *See* Tex. H.B. 71, 88th Leg., Reg. Sess. (2023), https://capitol.texas.gov/BillLookup/History.aspx?LegSess=88R&Bill=HB71.

or third party used for the purpose of satisfying a request or event," "include[ing] records from mortgage, education, and employment entities." Section 129B.001(7).

One popular method of "commercial" age verification relies on a user authorizing temporary charges on a credit or debit card. This is likely a permitted method under Section 129B.003(2)(B). Section 129B.003(2)(B) also likely permits methods that rely upon checking or analyzing third-party databases. These databases may contain identifying information about a website visitor based on "records from mortgage, education, and employment entries," credit checks, or advertising profiles built from third-party signal analysis of a user's browsing data, IP address, and social networks.

Age verification by biometric scanning (such as when a website visitor uploads a picture of his face or a recording of her voice and the website analyzes this information to estimate the visitor's age) "is gaining popularity as an age-gating and verification method."[4] While it is unclear if age verification by biometric scanning relies on "private transactional data" as defined by Section 129B.003(b)(2)(B), we discuss it here because it is among the most prevalent forms of online age verification and because the Fifth Circuit, below,

---

[4] *See* Sarah Forland, Nat Meysenburg & Erika Solis, *Age Verification: The Complicated Effort to Protect Youth Online*, New America 20 (Apr. 23, 2024), https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/challenges-with-age-verification/.

opined that "facial appearance" is one method allowed by Section 129B.003(b). App. 11a.

Finally, some websites collect information about a user based on the user's interactions with the website (such as browsing data, IP address, search history, location history, and information shared on social media networks) and then use that information to estimate the user's age.[5] Section 129B.003(2)(B) conceivably permits age verification by this kind of first-party signal analysis if it were determined to be a "commercially reasonable method" of estimating age.

Some websites may choose to use a combination of these methods to verify ages. Each of these potential methods is discussed in more depth below.

II. Existing Age Verification Technologies Are Often Ineffective and Present Privacy and Security Risks.

A. Uploading a Government-Issued ID

A prevalent method of online age verification requires a website visitor to upload a copy of a government-issued ID. First, the website must determine that the visitor is attempting to access the website from Texas. Next, it prompts the visitor to scan or photograph their government-issued ID and upload it

---

[5] *See, e.g.* Erica Finkle et al., *How Meta uses AI to better understand people's ages on our platforms* (June 22, 2022), https://tech.facebook.com/artificial-intelligence/2022/06/adult-classifier/.

to the website the visitor is attempting to access (or, in most cases, to a third-party verifier service contracted by the website). Some, but not all, age verification contractors may take an additional step of requiring the visitor to take and upload a picture of the visitor's face (i.e. a "selfie"). The website or third-party verification contractor then receives the copy of the user's ID. Different verification providers provide different degrees of analysis of the file to determine its authenticity and the age of the person to whom the ID was issued. If a selfie is uploaded, the service may use machine learning technology to estimate whether the selfie likely depicts the same person whose photo appears on the government ID. Based on this analysis, the website either grants or denies access. If an age verification contractor is used, that entity sends some information to the regulated website indicating whether the user is permitted to access the website.

For example, Veriff, an identity verification company, offers an age validation service that relies exclusively on a government-issued ID.[6] According to Veriff, this service involves three steps to ensure "[p]rotection and safety": First, "Veriff extracts the date of birth from your user's identity document to calculate their age."[7] Second, "[t]he calculated age is cross-checked to see if it is above your predefined minimum age threshold."[8] Third, "[t]he age validation

---

[6] *See, e.g.*, Veriff, *Age Validation*, https://www.veriff.com/product/age-validation (last visited Sept. 19, 2024).

[7] *Ibid.*

[8] *Ibid.*

result is returned and users below your predefined threshold can be automatically declined."[9] Another company, Yoti, offers a similar age verification service that require visitors to upload a selfie in addition to their government ID in order to cross-reference the two against each other.[10]

1. Effectiveness

This method of age verification is effective only if (1) the website accurately identifies every visitor in Texas, (2) the uploaded file purporting to be a government ID of a non-minor belongs to the visitor who uploaded it (sometimes requiring the upload of a selfie and verifying the two images are of the same person), (3) the ID is authentic, and (4) the verification service accurately identifies the date of birth on the ID. Accordingly, "there are many workarounds that underage users can use to circumvent" online age verification methods that rely on government IDs.[11]

---

[9] *Ibid*.

[10] *See, e.g.,* Declaration of Richard I. Sonnier III in Support of Plaintiffs' Motion for Expedited Preliminary Injunction, *Free Speech Coalition, Inc. v. Paxton*, No. 1:23-cv-00917-DAE (W.D. Tex. August 4, 2023), ECF No. 5-2 ("Sonnier Decl."), at ¶ 15, Table 2.

[11] *See, e.g.*, Daniel Castro, Information Technology & Innovation Foundation, *Protecting Children Online Does Not Require ID Checks for Everyone* (November 21, 2023), https://itif.org/publications/2023/11/21/protecting-children-online-does-not-require-id-checks-for-everyone/ ("ITIF *Protecting Children*"); *see also* Youssef A. Kishk*, State-Based Online Restrictions: Age-Verification And The VPN Obstacle In The Law*," 2 Int'l J. L. Ethics

First, minors can "use tools like virtual private networks (VPNs) to bypass age verification" by disguising their location to appear as though they are not logging on from Texas.[12]

Second, online age verification by government ID can be circumvented by borrowing, scanning, or purchasing images of the ID of another person older than 17. Some age verification services attempt to mitigate this weakness by checking an uploaded government ID against an uploaded selfie to estimate whether the selfie and the government ID belong to the same person. But, as we discuss below, selfies can also be spoofed, such as by holding up a photograph or image of another person's face to the smartphone camera or webcam.

Third, the method is ineffective when it fails to recognize whether the uploaded image is a copy of a government-issued ID that indicates an age above seventeen. "[E]nterprising teens can easily find various tools and instructions online to create a fake scanned image of an ID card."[13] And the extent of analysis that most commercial online age verification service-providers perform on an uploaded

---

Technology 150 (2024) at 137, https://www.doi.org/10.55574/VBDM8223. (By using VPNs, "minors could still access restricted harmful material without age-restrictions blocking them[.]").

[12] Sarah Forland et al., *supra* note 4 at 23; *see also* ITIF *Protecting Children*, *supra* note 11.

[13] ITIF *Protecting Children, supra* note 11.

government-issued ID is unclear. For example, the verifier could simply grant access upon receiving any file that looks like a government-issued ID with an appropriate age or it could take further steps to verify the ID against a third-party database or known IDs. Some age verification services appear to do little more than "extract[] the date of birth from [a] user's identity document," meaning that the authenticity of the ID is not verified by the age verification service.[14]

Finally, this method is ineffective for users who do not have government-issued IDs or a convenient method of scanning it, such as a smartphone camera or webcam. This matters: Researchers analyzing data from the 2020 American National Election Studies estimated that "[n]early 29 million voting-age U.S. Citizens did not have a non-expired driver's license and over 7 million did not have any other form of non-expired government issued photo identification."[15] Certain communities of citizens are more likely to lack government-issued IDs than others. "Nearly 3.1 million young people" (aged 18–29-years-old) "did not have any non-expired government issued photo ID in 2020," and within this group, individuals who were "18- or 19-years old were especially unlikely to have

---

[14] *See, e.g.*, Veriff, *Age Validation*, https://www.veriff.com/product/age-validation (last visited Sept. 19, 2014).

[15] Michael J. Hammer & Samuel B. Novey, *Who Lacked Photo ID in 2020?* 2-3, Center for Democracy and Civil Engagement (Mar. 13, 2023), https://www.voteriders.org/wp-content/uploads/2023/04/CDCE_VoteRiders_ANES2020Report_Spring2023.pdf.

any photo ID[.]"[16]. Racial and ethnic minorities also disproportionately lack IDs: Among voting-age citizens, "24% of Hispanic, 21% of Black, 12% of Native American, Native Alaskan, or another race, 9% of Asian, Native Hawaiian, and other Pacific Islanders . . . did not have a driver's license."[17]

Other people who are less likely to have current government issued IDs include undocumented immigrants, persons with disabilities, people experiencing homelessness, people who do not drive motor vehicles, people who have experienced theft, people who have recently moved, and people who have recently changed their name, for example, after becoming married.[18] These populations are not trivial. For instance, a recent Pew Research Center study found that Texas is home to 1.6 million undocumented immigrants.[19]

---

[16] *See id.* at 2–3.

[17] *Id.* at 4.

[18] Jillian Andres Rothschild, Samuel B. Novey & Michael J. Hammer, *Who Lacks ID in America Today?" An Exploration of Voter ID Access, Barriers, and Knowledge*, Center for Democracy and Civic Engagement (Jan. 2024), https://cdce.umd.edu/sites/cdce.umd.edu/files/pubs/Voter%20ID%202023%20survey%20Key%20Results%20Jan%202024%20%281%29.pdf.

[19] Ali Juell, *New Study: Texas' undocumented immigrant population remained relatively stable in 2021*, The Tex. Trib. (Nov. 21, 2023), https://www.texastribune.org/2023/11/21/texas-immigrants-pew-research/.

2. Security and Privacy Risks

The use of government-issued IDs to verify age introduces significant security and privacy concerns because it requires the transmission of all the identifying information on a government-issued ID paired with information about the website the visitor is attempting to access to websites that may not have the resources to handle data securely, may be located abroad and not practically subject to U.S. law, or may even be set up as scams to collect ID information for theft or sale using the Texas law as a pretense.

Digital copies of government-issued IDs are themselves a valuable asset for thieves, hackers, and hostile foreign governments.[20] When this information is paired with an individual's sensitive website visits—including, for example, site visits that could reveal a person's sexual orientation, pregnancy status, or reproductive health decisions—such data also becomes a target for crimes such as extortion.[21] Other than the non-retention requirement of Section 129B.002(b), which we discuss in greater detail below, HB 1181 imposes no other duty on the website operator, age-

---

[20] *See, e.g.,* Ramon Antonio Vargas, *Every Louisiana driver's license holder exposed in colossal cyber-attack,* The Guardian (June 16, 2023, 12:21 EDT), https://www.theguardian.com/us-news/2023/jun/16/louisiana-drivers-license-hack-cyber-attack(noting that "Russia-linked group claims responsibility for hack").

[21] *See* Michael Smith et al., *Browser history re:visited*, 12th USENIX Workshop on Offensive Technologies (2018), https://www.usenix.org/conference/woot18/presentation/smith.

verifiers, third parties, or intermediaries to secure a visitor's "identifying information" from accidental disclosure or data breach when stored, analyzed, or transmitted.[22]

In addition to the data breach risk, sensitive data obtained from government IDs may also *purposefully* be made available to third parties. HB 1181 does not prevent the entities that "perform[ ] the age verification" from transmitting or even selling the commercially valuable data obtained from a visitor's government IDs and browsing activity to commercial data brokers or advertising firms. *See* Section 129B.002(b) (requiring entities that "perform[ ] the age verification" to "not retain any identifying information of the individual"). And HB 1181 offers *no protections* for website visitors from the retention, transmission, or sale of their data by other entities that obtain their data but do not perform the age verification.[23] For

---

[22] Texas Data Privacy and Security Act requires companies to provide users notice it is processing certain kinds of personal data and gives consumers certain opt-out rights. Tex. Att'y Gen., *Texas Data Privacy and Security Act,* https://www.texasattorneygeneral.gov/consumer-protection/file-consumer-complaint/consumer-privacy-rights/texas-data-privacy-and-security-act , (last visited Sept. 17, 2024). However, these requirements apply only to "biometric data" (not including a photo, video, or audio recording) and certain kinds of "sensitive data". While this statute may apply to certain ID documents (such as driver's licenses noting visual impairment), it creates no private right of action and can only be enforced by the Texas Attorney General.

[23] *See id.*

example, as the trial court found, "any intermediary between the commercial websites and the third-party verifiers [that obtains the visitors' identifying information and/or browsing activity] will not be required to delete the identifying data." App. 126a.

B. Authorizing Temporary Credit or Debit Card Charges

Some websites attempt to verify a visitor's age by placing an "authorization hold" on a credit or debit card account. For example, YouTube relies on credit card information to verify the ages of some European visitors.[24] While this process typically happens in seconds, it requires transferring sensitive information through multiple platforms.

When card charges are used online to verify a visitor's age, the visitor is typically asked to fill out an authorization form to give a website permission to charge their card. Users will typically enter the following information: cardholder name, billing address, and zip code; card number, network (i.e., Visa, Mastercard), expiration date, and card verification value (CVV) code; and a statement authorizing the charge.

Then, the website or age verification vendor asks the bank to authorize a small charge. The issuing bank or card company then reviews the cardholder's

---

[24] *See Using technology to more consistently apply age restrictions,* YouTube Official Blog (Sept. 22, 2020), https://blog.youtube/news-and-events/using-technology-more-consistently-apply-age-restrictions/.

account and approves or denies the charge. Based on the information provided by the bank, the website can choose to allow or deny access to certain content.

1. Effectiveness

This method of age verification is generally ineffective because possession of a credit or debit card does not guarantee that an individual is over the age of 18.

While the Credit Card Accountability Responsibility and Disclosure Act of 2009 (CARD Act), 15 U.S.C. §§ 1601-1667f, 1681 *et seq.*, generally requires a consumer in the United States be over the age of 21 to be issued a credit card, that does not mean that only those 21 and older can authorize credit and debit card transactions. To begin, many credit card issuers allow the primary account holder to add a child as an authorized user to make purchases on the credit card account, often by using a card with the same card number and CCV as the adult's card.[25] This may allow children to access websites despite a credit check.

Moreover, many banks allow minors to have their own debit cards, if sponsored by adults.[26] Minors can

---

[25] Toni Perkins-Southam & Caroline Lupini, *Can I Add My Child To My Credit Card?*, Forbes Advisor (Jan. 11, 2024, 4:59 PM), https://www.forbes.com/advisor/credit-cards/should-you-add-your-children-as-authorized-user-on-your-credit-card/.

[26] *See* Bethany Hickey, *Best credit cards for teens under 18,* Finder (Sept. 4, 2024), https://www.finder.com/kids-banking/credit-card-options-teens.

also access prepaid credit cards without parental consent if purchased at a convenience store, online, or received as gifts.[27] Accordingly, the ability to fill out the information in a credit card authorization form is not sufficient to establish that the person is above the age of 18.

This age verification method is also overinclusive and, thus, may prevent individuals over the age of 18 from accessing content they are legally permitted to view. The FDIC reported that in 2021 approximately 5.9 million U.S. households were "unbanked," meaning that no one in the household had a checking or savings account at a bank or a credit union.[28] In fact, the FDIC found that more than a quarter of U.S. households lacked any credit card.[29]

2. Security and Privacy Risks

This method of age verification is also inherently risky. Authorizing a card transaction requires users to go through the same steps they would to complete any online transaction: upload personally identifiable information alongside payment information. When

---

[27] Jackie Snow, *Why Age Verification Is So Difficult for Websites*, Wall Street J. (Feb. 27, 2022, 8:00 am ET), https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728?st=f0lp8y2cgptjoyb&reflink=article_email_share.

[28] F.D.I.C., *2021 FDIC National Survey of Unbanked and Underbanked Households, 2021 Executive Summary*, (Oct. 2022).

[29] *Id.* at 6.

used for age verification, this already valuable information is paired with the user's potentially sensitive browsing history and sent to any website with content meeting the statutory criteria, including those set up for the purpose of gathering credit card information under the guise of complying with Texas law.

Disclosing such information to any third party also presents a general privacy risk. Financial institutions or payment processors will obtain information linking the identity of the cardholder with the website they attempt to access. These vendors are not obligated to delete this information under HB 1181 and could sell it to advertisers or other third parties, as financial institutions commonly do. For example, one common credit card company was found routinely to "sell[ ] cardholder transaction data through third party online data marketplaces and through its in-house Data & Services division, giving many [other] entities access to data and insights about [its] consumers at an immense scale."[30] This could be true regardless of whether the financial institution were found to "perform[ ] the age verification" under Section 129B.002(b) because HB 1181 does not prohibit entities from transferring or selling information obtained from age verification methods. Once data is sold or re-used for advertising purposes, it may be revealed to many other parties. For example, targeted advertising based on a user's visit to a pornography

[30] Public Interest Research Group, *How Mastercard sells its 'gold mine' of transaction data*, (Updated June 17, 2024), https://pirg.org/edfund/resources/how-mastercard-sells-data/.

site may be displayed on the device that was used to visit the website or service, revealing the visit to friends or family members.

C. Third-party Databases and Analysis

Some third-party services provide age verification by assembling databases that allow them to match certain personal identifying information to an estimated age. The user will input some identifying information to the website, such as a mobile number. The website then queries that information against those third-party databases, which requires sending the identifying information to the third party. The third-party then reports an estimated age to the website, which grants or denies access to the user based on the age reported by the third-party. Some examples of these programs include VeriMe, which uses a customer's mobile phone number; AgeChecker, which uses a customer's date of birth; Melissa, which uses a customer's address; and Equifax and Experian, which check information entered by a customer against their credit database. See Sonnier Decl. at para. 15.

1. Effectiveness

These methods are both ineffective at ensuring exclusion of children and ineffective at ensuring access for adults. First, these third-party platforms require the user to provide accurate identifying information that is unique to them in the first instance. As a consequence, a minor may be able to intentionally deceive the system by submitting information belonging to an adult. Inversely, if an adult has recently

moved or changed phone numbers, they may enter accurate information that the system cannot verify. Second, this method relies on the user having access to the verification data required, whether it is a phone number, home address, or driver's license. It also requires the user's information to be in the specific database queried. If a user's information is not included, for example because they recently turned 18, lack state identification, or do not have a cell phone number, they may be blocked from accessing content they have a constitutional right to access.

2. Security and Privacy Risks

This method of verification relies on third parties building robust databases that match identifying information to estimated ages. It therefore creates a market for amalgamating large quantities of personally identifiable information about consumers.

In addition, the greater the number of third-party systems introduced in the verification process, the greater the chance for security vulnerabilities. Hackers frequently target the weakest links in the chain of digital vendors. These so-called "supply chain" data breaches rely not on hacking a website itself, but on hacking third-party vendors in an organization's supply chain. Harvard Business Review found that 98% of organizations have a relationship with a vendor that experienced a data breach within the last two years.[31]

---

[31] Stuart Madnick, *Why Data Breaches Spiked in 2023*, Harvard Bus. Rev. (Feb. 19, 2024), https://hbr.org/2024/02/why-data-

Third-party age verification vendors will also then be aware of which websites are sending age verification requests about which individuals. As noted above, the third-party database is not clearly subject to the non-retention requirement of HB 1181. HB 1181 does not prohibit age-verification vendors from transmitting or even selling user data. *See* App. 126a.

D. Biometric Scanning

Other age verification providers rely on artificial intelligence to analyze biometric data such as a photo, video, or voice recording to guess at a website visitor's age like a carnival worker might. These providers train machine learning algorithms on datasets that pair images of faces or recordings of voices with the age of the source of the image or recording.[32] When a visitor wants to access a website that uses biometric scanning, the visitor collects and uploads a sample of their biometric identifiers (typically a selfie taken from their phone). The website or third-party service performing verification then receives the copy of the user's biometric scan. Different verification providers provide different degrees of analysis of the file to estimate the age of the person represented by the biometric scan and whether the biometric scan is

---

breaches-spiked-in-2023.

[32] Rachel Metz, *A reporter tried the AI Instagram wants to use to verify age. Here's what it found,* CNN Business (June 27, 2022, 7:30 PM), https://www.cnn.com/2022/06/27/tech/instagram-ai-age-estimation-face-scan/index.html.

authentic.[33] If a third-party verifier is used, that entity sends information to the website indicating about the estimated age, which the website can then use to decide whether the user is permitted to access the website.

1. Effectiveness

Biometric scanning is by its nature imprecise, especially inaccurate for certain populations, typically requires the exclusion of young adults, and often can be circumvented.

First, age estimation from biometric scanning is probabilistic and, accordingly, can only give estimated age within ranges. "Age estimation algorithms . . . [involving] facial image analysis . . . have been studied extensively in machine learning research[.]"[34] That research reveals that biometric scanning cannot be used to precisely identify a website visitor's age, leading some researchers to conclude that

---

[33] Jennifer Bryant, *The 'growing ecosystem' of age verification,* Intl. Assoc. of Privacy Pro. (Mar. 28, 2023), https://iapp.org/news/a/the-growing-ecosystem-of-age-verification.

[34] Zahra Stardust et al., *Mandatory age verification for pornography access: Why it can't and won't 'save the children,'* Big Data & Soc'y 5 (2024) at 5, https://journals.sagepub.com/doi/pdf/10.1177/20539517241252129 (citing H. Otto et al., *Age estimation from face Images: Human vs. machine performance*, IEEE IAPR Int'l Conference on Biometrics, Madrid, Spain (June 4-7, 2013), https://doi.org/10.1109/ICB.2013.6613022).

contemporary "age estimation algorithms . . . lack . . . suitability for restricted access systems."[35] One problem is that "the indicators programmed into software often rely on stereotypical indicators of age," such as the presence of wrinkles, hairline distributions, and "distance ratios of facial features with respect to each other (for instance, the lengthening of a subject's jawline with respect to their upper lip)."[36] But these "indicators are highly variable."[37] As a result, current age-estimation approaches "are . . . susceptible to misclassification by generalising that certain . . . features belong to a certain age group" when this is not true in all cases.[38]

Second, for several reasons, the accuracy of age estimation by biometric scan "is strongly influenced by algorithm, sex, image quality, region-of-birth, age itself, and interactions between those factors."[39] First, many "indicators" used to estimate age vary significantly across different populations. For example, craniofacial growth ratios have been found to "vary with ethnicity," but age-estimation algorithms "do not acknowledge such contextualisations," leading to less

---

[35] *Id.* at 4.

[36] *Ibid.*

[37] *Ibid.*

[38] *Ibid.*

[39] Kayee Hanaoka et al., *Face Analysis Technology Evaluation: Age Estimation and Verification*, National Institute of Standards and Technology, U.S. Dept. of Commerce (May 2024), at 1, https://doi.org/10.6028/NIST.IR.8525.

accurate results.[40] As another example, analysis of facial hair distribution "has been proven to . . . skew age estimation" because "[d]istributions of facial hair are also highly variable across different populations," such as people of different sex, gender, and people having certain medical conditions.[41] Second, "[e]xisting facial recognition technologies are usually trained on data sets that are biased towards white faces with significant under representation of non-white faces, which limits their applicability among the general population[.]"[42] Researchers have found that common facial recognition algorithms "performed better on male faces than female faces (8.1%-20.6% difference in error rate)," "better on lighter faces than darker faces (11.8%-19.2% difference in error rate)," and "worst on darker female faces (20.8%-34.7% error rate)."[43]

Third, because age estimation by biometric scanning is inherently imprecise, commercial age verification providers typically recommend that their clients build in a "buffer" to increase compliance with age verification laws. The U.S. Department of Commerce recently reported that for age verification providers targeting an age of 18 years, "a seven year buffer is conventional," meaning that adults estimated to be between eighteen and twenty-five may be required to

---

[40] *See* Zahra Stardust, *supra* note 15, at 4.

[41] *Ibid.*

[42] *Ibid.*

[43] *Id.* at 4-5.

provide additional information to verify their age.[44] Last year, popular age verification provider Yoti "suggest[ed] a buffer of 3–5 years as an appropriate buffer for highly regulated sectors," such as "adult content," "for the 13-25 age band."[45]

Finally, age verification by biometric scanning can be circumvented. Recent research confirms that "easy-to-perform attacks, like replaying a video or displaying a photo to the camera, can easily spoof state of the art face recognition."[46] And "attacks on age verification [algorithms are even] harder to detect." "[I]t is easier to perform attacks on age verification [than mere facial recognition], since one can use any photos from [the] internet to perform an attack."[47] Moreover, "de-aging/aging or other AI-based filters … common in social media apps … can be used to change the appearance of a face to make it look younger or older."[48] And "age verification systems are built to detect mostly children, while children data is practically

---

[44] *See* Hanaoka *supra* note 39 at 22.

[45] Yoti, *Yoti Facial Age Estimation* (Dec. 2023) at 16, https://www.yoti.com/wp-content/uploads/2024/04/Yoti-Age-Estimation-White-Paper-December-2023.pdf.

[46] Pavel Korshunov et al., *Vulnerability of Face Age Verification to Replay Attacks* 1-2, IEEE International Conference on Acoustics, Speech, and Signal Processing (2014),https://publications.idiap.ch/attachments/papers/2024/Korshunov_ICASSP_2014.pdf.

[47] *Id.* at 2.

[48] *Id.*

absent in the datasets on which [presentation attack detection] systems designed for biometrics are trained on."[49] Indeed, one researcher was able to fool an online age estimator by holding a pet dachshund in front of his face.[50] The service reported an estimated age of 42-46.[51]

2. Security and Privacy Risks

Age verification by biometric scanning shares many security and privacy concerns with age verification by government ID. For example, linking individuals' biometric scans to their browsing activity creates a tempting target for thieves, hackers, and hostile foreign governments.[52]

---

[49] *Id.*

[50] Chelsea Jarvie and Karen Renaud, *Are you over 18? A Snapshot of Current Age Verification Mechanisms* 12, Proceedings of 2021 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop (2021), https://strathprints.strath.ac.uk/82540/ (Ex. D to the Sonnier Decl. (ECF 5-2, at 54)).

[51] *Ibid.*

[52] *See, e.g.,* Andy Greenberg, *OPM Now Admits 5.6m Feds' Fingerprints Were Stolen By Hackers*, Wired (Sep. 23, 2015, 11:30 AM), https://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers/ (noting that hack compromising data of up to 21.5 million federal employees, including intelligence and military employees with security clearances, likely originated in China); *see also FTC Warns About Misuses of Biometric Information and Harm to Consumers,* F.T.C. Press Release (May 18, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-

Age verification by biometric scanning exacerbates these security and privacy concerns due to the nature of biometric data. Biometric data describes characteristics that are intimately connected to a particular individual. This means, *first*, it cannot truly be anonymized. Aside perhaps from identical twins, no two people have the same facial structure, retina appearance, or voice patterns. So, to the extent it is accurate, biometric data identifies a single person in a way that a name or date of birth does not. Second, biometric data is often immutable. So, while one can change or deactivate a password, email address, or credit card number that has been hacked or subject to a data breach, one cannot change their facial structure or voice patterns to mitigate further injury from its release.[53] This makes collection, transmission, and/or storage of biometric data especially risky.[54]

E. First-party Signal Analysis

Another current method of age verification is "first-party signal analysis," commonly used by social media websites to verify the ages of their users. This

---

biometric-information-harm-consumers.

[53] *See, e.g., id.*

[54] As the World Bank has explained, "no system [for securing biometric data] is foolproof," since "even if biometrics are stored as encrypted templates . . . , there is still the possibility that synthetic biometric images can be reconstructed from templates." *Biometric Data, ID4D Practitioner's Guide: Version 1.0*, World Bank (October 2019), https://id4d.worldbank.org/guide/biometric-data.

method requires platforms to rely on data that the users generate on the platform to determine their age.

For example, Meta Platforms, Inc. (Facebook and Instagram's parent company) estimates whether someone is eighteen through first-party signal analysis, and intends to roll out such technology to estimate whether users are thirteen (and remove their profiles from the website).[55] Artificial intelligence is used to review and identify posts signaling age (such as a post wishing a user "Happy 21st Birthday!") to compare to the ages that users list across linked apps and with user browsing data of others in a similar age category.[56]

In other cases, these websites use cookies or IP address recognition to associate the user's current visit with data from previous visits. The website then compares that with data it collects about the visitor, data it collects from other visitors, and data from third-party databases to estimate the age of the visitor.

1. Effectiveness

This method offers only a probabilistic estimate of age. Further, this method's effectiveness depends on the website linking a user's visit to the website to

---

[55] Pavni Diwanji, *How Do We Know When Someone Is Old Enough to Use Our Apps?,* Meta Newsroom (Jul. 27, 2021); https://about.fb.com/news/2021/07/age-verification/

[56] *Id., see also* Finkle et al., *supra* note 5.

previous visits to the website. This may not work if the user has disabled cookies, if the user's browser that blocks cross-site tracking or fingerprinting, if multiple users visit the website from the same IP address, or if the user has never visited the website before.

2. Security and Privacy Risks

In its current use by social media platforms, this method relies on large amounts of user data already stored by the platforms – and linked to the data social networking platforms already have about user social contacts. Using this method to verify ages on websites containing allegedly "sexually harmful" material may not be feasible since they often will not have access to such large qualities of user data (or may not be able to retain it under HB 1181's non-retention requirement). It also may encourage websites to ask or compel users to log in with or link their activity to their social media accounts, which could potentially reveal to the social media platform what sensitive websites an adult user is visiting, or to provide the user's social media data to the website or its age verification vendor.

III. The Ineffectiveness of Current Age Verification Methods, Combined with the Technologies' Security and Privacy Risks, Unconstitutionally Burden Adults' Access to Constitutionally Protected Speech and Render HB 1181 Both Under and Overinclusive.

As Petitioners explain, this Court has held that laws imposing content-based burdens on adults' access to constitutionally protected content are subject to strict scrutiny. *Reno v. ACLU,* 521 U.S. 844, 874 (1997); *Ashcroft v. ACLU,* 542 U.S. 656, 665-66 (2004). The limits of the technology currently available to satisfy HB 1181's age verification requirements (discussed *supra*) will exacerbate the burden to adults' access to protected content without achieving the government's objective of protecting children.

A. Implementing HB 1181 With Current Technology Will Necessarily Prevent Some Adults from Accessing Some Protected Content Altogether.

No matter what method(s) a website uses for age verification, some adults will be unable to access the site. Many adults do not have a government ID or bank account, *supra* II.A-B, and thus will be unable to access websites that offer only those methods of age verification.

For those sites that use AI-biometric age estimation, as noted, *supra* at II.D.2, "a seven year buffer is conventional," meaning that adults estimated to be between eighteen and twenty-five in particular will

either be denied access or be required to provide additional information – normally a government ID – to verify their age.[57] Individuals in that buffer age group without government ID may be left without a way to access the protected content. And first-party signal analysis may work only for a limited number of sites such as social media platforms.[58]

These technological limitations will completely bar some adults' access to protected content, rendering the legislation significantly overinclusive.

B. The Security and Privacy Risks Associated with Current Technologies–Including That Sensitive Browsing Activity Will Be Deanonymized–Also Burdens Adults' Access to Protected Content.

The security and privacy risks of current age verification technologies further burden adults' access to protected content. Under the existing methods permitted by HB 1181, a website cannot verify a user's age without obtaining identifying or similarly sensitive information. As a result, HB 1181 forces adults to take on significant risks to their privacy and

---

[57] *See* Hanaoka, *supra* note 39 at 22.

[58] *See, e.g.* Marley Malenfant, *What is the SCOPE Act? New Texas law requires parental approval over kids' social media,* Austin American-Statesman (Sept. 13 .2024), https://www.statesman.com/story/news/state/2024/09/13/scope-act-texas-hb-18-social-media-children-personal-data-online-judge-robert-pitman-block/75178891007/.

anonymity to access protected material, which will act as a deterrent to doing so.

As discussed above, the information users provide for age verification is subject to unauthorized disclosure through data breaches. Indeed, some of the companies that offer to perform age verification services permitted under HB 1181 have already been hacked. AU10TIX, a company which specializes in various identity verification services including age verification, left login credentials exposed online *for over a year*," "potentially compromis[ing] the personal information of millions of users, including facial images and driver's licenses.[59] Equifax and Experian too advertise age verification services[60]—and have also been breached, exposing the personally identifying information of millions of individuals.[61]

---

[59] Jason Kelley, *Hack of Age Verification Company Shows Privacy Danger of Social Media Laws,* Electronic Frontier Foundation (June 26, 2024), https://www.eff.org/deeplinks/2024/06/hack-age-verification-company-shows-privacy-danger-social-media-laws (emphasis added).

[60] Equifax, *Age Verification,* https://www.equifax.co.uk/business/age-verification/en_gb/ (last visited Sep. 17, 2024). Experian, *Age verification services for your business*, https://www.experian.co.uk/business/regulation-and-fraud/identity-checks/age-verification (last visited Sep. 17, 2024).

[61] F.T.C., *Equifax Data Breach Settlement*, F.T.C. (Feb. 2024), https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement; *AG Healey Secures $16 Million from Multistate Settlements with Experian and T-Mobile Over Data Breaches*, Mass. Office of the Att'y Gen. Press Release (Nov. 7, 2022),

In addition to the risk of a data breach, as discussed above, nothing in the statute precludes a variety of entities from selling users' identity data to advertisers, data brokers, or other third parties. And the statute creates a pretense for bad actors to set up pornography and similar sites for the purpose of collecting users' credit card or other information, ostensibly for age verification but in reality for criminal purposes.

These risks are exacerbated by the fact that a user's identity information will be associated with their browsing behavior. Attaching one's identity to the site a user is visiting could, for example, reveal information about the user's sexual orientation or sexual preferences or simply result in embarrassment. The sale of browser history data is widespread. "Although [some] platforms claim data is anonymized," Oxford University researchers have shown that anonymization "is actually very hard to do in practice; you only need two or three data points to identify somebody."[62] This data has been sorted to "target judges, elected officials," and "military personnel."[63] Indeed, cybercriminals have already targeted

---

https://www.mass.gov/news/ag-healey-secures-16-million-from-multistate-settlements-with-experian-and-t-mobile-over-data-breaches.

[62] Cristina Criddle, *Web browsing data collected in more detail than previously known, report finds*, Financial Times (Nov. 13, 2023), https://www.ft.com/content/6c8f1f24-b690-4bbd-b726-28b2d6f10800.

[63] *Id.*

this kind of information.[64] The FTC has warned of growing risks of scams threatening to blackmail internet users with threats to reveal their browsing history.[65] The White House has warned of similar threats to foreign security.[66]

The range of privacy and security risks, coupled with the loss of anonymity about visits to pornography or other sensitive sites, will heavily burden adult access to protected information.

---

[64] *See, e.g.,* Daniel Victor, *The Ashley Madison Data Dump, Explained*, N.Y. Times (Aug. 19, 2015), https://www.nytimes.com/2015/08/20/technology/the-ashley-madison-data-dump-explained.html; Samuel Gibbs, *Adult Friend Finder and Penthouse hacked in massive personal data breach,* The Guardian (Nov. 14, 2016), https://www.theguardian.com/technology/2016/nov/14/adult-friend-finder-and-penthouse-hacked-in-largest-personal-data-breach-on-record.

[65] Bridget Small, F.T.C, *Consumer Alert: Scam emails demand Bitcoin, threaten blackmail,* FTC Consumer Advice (Apr. 29, 2020), https://consumer.ftc.gov/consumer-alerts/2020/04/scam-emails-demand-bitcoin-threaten-blackmail.

[66] White House, *FACT SHEET: President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data* (Feb. 28, 2024), https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/.

C. HB 1181 Will Also Fail to Achieve its Purpose of Protecting Children Because They Can Easily Circumvent Current Age Verification Technologies.

Many forms of age verification, such as biometric scanning, probabilistic analysis of third-party databases, and first-party signal analysis are imprecise. As described *supra*, each age verification method has significant disadvantages that are compounded for certain Americans, including those in lower income groups who are less likely to have access to formal government identification, the technology to provide biometric data easily, or credit cards, and individuals from less-represented racial and ethnic groups who are less likely to be correctly aged by biometric measures.

Further, many forms of age verification technology are easily circumvented. Government-issued ID scans can be bypassed when children use falsified IDs by altering images of such identification.[67] Users can defeat biometric scanning by using deepfakes to bypass video or voice "liveness" checks—technology which is becoming increasingly available.[68] Minors

---

[67] Clare Y. Cho, Cong. Rsch. Serv., R47884, *Identifying Minors Online* (Jan. 2, 2024) at 5, https://crsreports.congress.gov/product/pdf/R/R47884.

[68] Jule Pattinson-Gordon, *Report: Biometric Injection Attacks on the Rise,* Government Technology (Mar. 15, 2024), https://www.govtech.com/security/report-biometric-injection-attacks-on-the-rise.

can borrow others' card information to bypass credit card checks. Minors can also avoid age verification checks altogether by using VPNs to appear as though they are visiting websites from other states.[69] But, problematically, free VPNs (as children may likely use) are more likely to either track and sell user data or insert malware into user's computers.[70]

D. HB 1181's Non-retention Requirement Is Insufficient to Address These Risks.

HB 1181 requires that the "commercial entity . . . or a third party that performs the age verification . . . may not retain any identifying information of the individual." Section 129B.002. But this "non-retention" requirement offers little protection for the security and privacy of website visitors' data.

First, HB 1181 does not define "performs the age verification," "retain" or "identifying information." As

---

[69] Shoshana Weissman & Canyon Brimhall, *Age-verification laws don't exempt VPN traffic. But that traffic can't always be detected*, R Street Institute (Aug. 29, 2023), https://www.rstreet.org/commentary/age-verification-laws-dont-exempt-vpn-traffic-but-that-traffic-cant-always-be-detected/.

[70] Toni Matthews-El et al., *Is Using a VPN Safe? What You Need To Know About VPN Security,* Forbes Advisor (June 1, 2024), https://www.forbes.com/advisor/business/software/are-vpns-safe/; *see also* Lauren Silverman, *Turning to VPNs for Online Privacy? You Might Be Putting Your Data At Risk,* NPR (Aug. 17, 2017), https://www.npr.org/sections/alltechconsidered/2017/08/17/543716811/turning-to-vpns-for-online-privacy-you-might-be-putting-your-data-at-risk.

a result, it is unclear who must delete "identifying information," exactly what must be deleted, and when.

Second, HB 1181 does not require every entity likely to receive sensitive data to delete it. HB 1181 does not prohibit transmission of data to third parties. Entities associated with the website or age verification companies that do not "perform[ ] the age verification" are not obligated to delete the information. For example, when an entity performing an age verification service runs a user's credentials against a database maintained by a third-party entity, it is not clear that the non-retention requirement applies to the third party. A third party that performs age verification services might create a second entity that does not perform age verification services, and then share data between the two entities to avoid the non-retention requirement. Intermediaries that receive sensitive data in transit between the user and the age verifier are also not obligated to delete the data.

Third, notwithstanding the non-retention requirement, HB 1181 appears to contemplate that some identifying information will be stored. Any verification method that requires checking someone's identity against "public or private transactional data" requires the existence of a database containing people's identities and ages. HB 1181 also contemplates granting the verifier with access to "digital identification," which is defined as certain "information stored on a digital network." Section 129B.003(a).

Fourth, while the law provides that the attorney general may elect to sue an entity that knowingly

violates HB 1181, including by "retain[ing] identifying information in violation of Section 129B.002(b)," Section 129B.006(a) & (b)(2), enforcement of the non-retention requirement faces several impediments.

It is unclear how the Attorney General would monitor every impacted website for compliance with the non-retention requirement. State governments often lack resources to effectively detect even large data breaches and generally rely on the breached parties to alert the government of a breach.[71] Here, in any event, enforcement would focus on the *absence* of data, rather than its existence, which is harder to discover. Thus, the Attorney General will likely only hear about noncompliance with the non-retention requirement in the event of a breach, when it is too late to protect users' privacy.

CONCLUSION

Technologists are working to develop age verification systems that protect user data and identification.[72] While these technologies are not yet mature,

---

[71] *See*, *e.g.,* Jonathan Greig, *More than 400,000 have data leaked in cyberattack on Texas education organization*, The Record (June 20, 2024), https://therecord.media/texas-atpe-educators-data-breach-notification, *see also* Att'y Gen. of Tex., *Data Security Breach Reports*, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited Sept. 17, 2024) (listing over 500 data breaches impacting Texans reported so far in 2024).

[72] Researchers have recently built an anonymous age-verification system by storing cryptographic proofs from ID providers on a

such development suggests that the goal of protecting children from harmful material without risking online security and privacy is possible to achieve.

However, using technology currently available, the Texas law does little to protect children from online pornography and presents significant privacy and security risks that will burden adult access to constitutionally protected content.

Respectfully submitted,

ANDREW S. BRUNS
Counsel Of Record
AMOS J. B. ESPELAND
COURTNEY J. LISS
IMARA MCMILLAN
KEKER, VAN NEST & PETERS, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: (415) 391-5400
Facsimile: (415) 397-7188
Counsel for Amici Curiae

September 20, 2024

---

shared public ledger through blockchain technology. In theory, cryptographers could develop "[a]nonymous credentials [that] allow someone to prove some fact about themselves (such as being at least 18 years old) without revealing their entire identity." Sarah Scheffler, *Age Verification Systems Will Be a Personal Identifiable Information Nightmare,* Communications of the ACM (June 10, 2024), https://cacm.acm.org/opinion/age-verification-systems-will-be-a-personal-identifiable-information-nightmare/#B1.