Case No. 25-00146

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

NETCHOICE,
Plaintiff-Appellant,

v.

ROB BONTA, in his Official Capacity as Attorney General of California
Defendant-Appellee.

Appeal from the United States District Court
for the Northern District of California
The Honorable Edward J. Davila, Presiding
Case No 5:24-cv-07885-EJD

BRIEF OF AMICUS CURIAE CENTER FOR DEMOCRACY & TECHNOLOGY IN SUPPORT OF PLAINTIFF-APPELLANT

ANDREW S. BRUNS, #315040
FLORA D. MORGAN, #359733
KEKER, VAN NEST & PETERS LLP
633 Battery Street
San Francisco, CA 94111-1809
Telephone: 415 391 5400
Facsimile: 415 397 7188

Attorneys for Amicus Curiae Center for Democracy & Technology

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, Amicus state it does not have a parent corporation and that no publicly held corporation owns 10% or more of its stock.

DATED: February 6, 2025

/s/ Andrew S. Bruns
Andrew S. Bruns

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Federal Cases

State Statutes

Other Authorities

INTRODUCTION AND INTEREST OF *AMICUS CURIAE*[1]

"[W]hatever the challenges of applying the Constitution to ever-advancing technology, the basic principles of the First Amendment do not vary." *Moody v. NetChoice, LLC*, 603 U.S. 707, 733 (2024) (citations and quotations omitted). Amicus Center for Democracy & Technology (CDT) aims to demonstrate how implementing the age verification requirements of California's Senate Bill 976 ("SB 976") will burden and potentially block adults' access to constitutionally protected speech while failing to achieve its goal of protecting children from the dangers of social media addiction.

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.

SUMMARY OF ARGUMENT

SB 976 prohibits operators of "addictive internet-based service[s] or application[s]" from providing access to certain features to a user known to be a minor, absent parental consent. The law requires operators of these services to verify the age of each user on their platform and to only allow adults, or children

[1] CDT certifies that all parties have consented to this brief's filing. 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 CDT or its counsel made any monetary contribution to this brief's preparation or submission.

with parental permission, to access those features. But the limitations of current age verification technology create an unjustifiably high burden to accessing this protected content.

Proponents of SB 976 argue that its requirements do not impact expression, because "engagement maximization" responds solely to user behavior and does not reflect editorial judgment about the underlying content. But decisions regarding how to order content, even if agnostic to the underlying content itself, reflect constitutionally protected editorial judgment. Moreover, SB 976 imposes content-based restrictions by limiting the ability of certain service providers to exercise their editorial discretion on the basis of the type of speech they publish.

In this brief, *Amicus first* describes how SB 976 restricts access to social media feeds and requires all users to submit personally identifiable and sensitive data to gain access.

Second, *Amicus* describes how current age verification methods are both insufficiently effective at their stated task and pose security and privacy risks to individuals that use them.

Third, *Amicus* explains that even if *some* kind of age verification is permissible under the Constitution, SB 976 is not narrowly tailored to achieve the government's interest of protecting minors. Instead, the law will burden adults'

access to protected content without furthering the government's objective of protecting children.

ARGUMENT

I. SB 976 Requires All Users to Divulge Volumes of Sensitive Personal Data.

SB 976 requires operators of so-called "addictive" internet-based websites, services or applications ("Operators") to verify the age of visitors before granting them access to certain core features. Cal. Health and Safety Code §§ 27000.5(b)(1), 27002(a)–(b). It requires Operators to "reasonably determin[e]" whether a user is a minor and restrict access for any user known to be a minor, unless they receive "verifiable parental consent." §§ 27001(a)(1)(B), 27006(b). The law leaves it to the Attorney General to outline further regulations "regarding age assurance and parental consent." § 27006(b).

Pursuant to SB 976, users known to Operators as minors (and those erroneously determined to be minors) will, by default, have access to so-called "addictive feeds"—streams of media powered by algorithms that display content based on information provided by or associated with the user—either restricted to one hour per day or programmed to exclusively display content to the user chronologically. § 27001(a). The definition of "addictive feeds" encompasses the core features of most social media platforms, including TikTok's "For You" Page and Facebook, Instagram, and X feeds. If not excluded by the law's exemptions,

SB 976 can be read to include media streaming services such as Spotify and Netflix.

SB 976 also prohibits Operators of "addictive feed" platforms from sending push notifications—alerts generated by a platform when it is closed, notifying the user of new activity—to users known to be minors during hours they would presumably be sleeping or in school. § 27002(a)—(b); Compl. 28:17-19.

On top of the limitations it imposes on user access, SB 976 also creates data-intensive reporting requirements. The law requires Operators to "annually disclose the number of minor users" of its platform, the number of minors "for whom the operator has received verifiable parental consent," and "the number of minor users as to whom the [access] controls [] are or are not enabled." § 27005.

In practice, the requirements of SB 976 would effectively mandate that *all* users of social media and streaming music and video platforms provide personal information to verify their age as a prerequisite to accessing key features of these platforms. The requirement that a minor must show "verifiable parental consent" to access certain features would necessitate the transmission and verification of even more personal data to verify the parent-child relationship and parental rights—e.g. a birth certificate or custody agreement—for such an exception to take hold.[2]

[2] *See Assembly Committee on Privacy and Consumer Protection* at 10 (July 2024), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=202320240SB976#.

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

While specific regulations governing the method of age verification required by SB 976 are forthcoming, the statute lacks necessary safeguards for implementing an "age gate"—a virtual checkpoint intended to block minors. All currently available alternatives are inaccurate and rely on some degree of personally identifiable data to identify a platform user's estimated age. *See Netchoice, LLC v. Bonta*, 2024 WL 5264045, at *2 (N.D. Cal. Dec. 31, 2024).

A. Biometric / Facial Scanning

One age assurance technology relies on artificial intelligence to analyze biometric data such as a user's photo, video, or voice recording to guess their age, like a carnival barker guessing the ages of fairgoers walking down the midway might. Technology 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.[3]

When a visitor wants to access a website that uses biometric scanning, the visitor collects and uploads a sample of their biometric identifier (typically a selfie taken from their phone). The website or third-party performing age assurance then

[3] 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.

receives the copy of the user's biometric scan. Different providers provide different degrees of analysis of the file to estimate the age of the person represented by the biometric scan and determine whether it is authentic.[4]

1. Effectiveness

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

First, age estimation from biometric scanning is probabilistic and, accordingly, can only give estimated age within ranges. Research of "[a]ge estimation algorithms . . . [involving] facial image analysis" reveals that biometric scanning cannot be used to precisely identify a website visitor's age, leading some researchers to conclude that contemporary "age estimation algorithms . . . lack . . . suitability for restricted access systems."[5] 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

[4] 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.

[5] 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 4-5, https://journals.sagepub.com/doi/pdf/10.1177/20539517241252129.

jawline with respect to their upper lip)."[6] But these "indicators are highly variable" making current age-estimation approaches "susceptible to misclassification by generalising that certain . . . features belong to a certain age group" when this is not true in all cases.[7]

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."[8] 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 accurate results.[9] 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[.]"[10] Researchers have found that common facial recognition

---

[6] *Id.* at 4.
[7] *Id.*
[8] 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.
[9] *See* Zahra Stardust, *supra* note 5, at 4.
[10] *Id.*

algorithms "performed better on male faces than female faces" "better on lighter faces than darker faces," and "worst on darker female faces."[11]

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, guaranteeing that the use of this technology will misclassify a significant number of adults. 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 25 and younger may need to provide additional information to verify their age.[12] Last year, popular age verification provider Yoti "suggest[ed] a buffer of 3–5 years as an appropriate buffer for highly regulated sectors" within the "13-25 age band."[13]

Finally, age verification by biometric scanning can be circumvented. While technology advancements in artificial intelligence have made biometric scanning more resistant to facial spoofing, it has also increased the ways a biometric scanner can be spoofed.[14] "[A]ttacks on age verification [algorithms are even] harder to

---

[11] *Id.* at 4-5.
[12] *See* Hanaoka *supra* note 8 at 22.
[13] 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.
[14] Faseela Abdullakutty, Eyad Elyan, and Pamela Johnston, *A review of state-of-the-art in Face Presentation Attack Detection*, Information Fusion, Nov. 2021, at 65-6, https://doi.org/10.1016/j.inffus.2021.04.015.

detect" because "filters … common in social media apps … can be used to change the appearance of a face to make it look younger or older." And "age verification systems are built to detect mostly children, while children data is practically absent in the datasets on which [presentation attack detection] systems designed for biometrics are trained on."[15] Indeed, one researcher was able to fool an online age estimator by holding a pet dachshund in front of his face.[16] The service reported an estimated age of 42-46.[17]

2. Security and Privacy Risks

Age estimation by biometric scanning raises many security and privacy concerns because linking individuals' biometric scans to their browsing activity creates a tempting target for thieves, hackers, and hostile foreign governments.[18]

---

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

[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/.

[17] *Id.*

[18] *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),

Age estimation by biometric scanning exacerbates these concerns due to the nature of biometric data. Industry experts and proponents argue that because age assurance scans do not attempt to identify the individual, they are not as intrusive as biometric scans that do seek to identify; however, any collection of biometric data—regardless of the purpose for which it is collected—can be used to identify a single person. Biometric data describes characteristics that are intimately connected to a particular individual and cannot be anonymized. Aside perhaps from identical twins, no two people have the same biometric markers. So, to the extent it is accurate, biometric data, even if it is not collected to link that data to a particular person, 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.[19] This makes collection, transmission, and/or storage of biometric data especially risky.[20]

---

https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers.

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

[20] 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.

B. First-party Signal Analysis

Another current method of age assurance is "first-party signal analysis," already commonly used by social media platforms to verify user age. Platforms using this method rely on their own user engagement data to estimate age.

For example, Meta Platforms, Inc. (Facebook and Instagram's parent company) estimates whether someone is 18 through first-party signal analysis, and intends to use this technology to estimate whether users are 13 (and remove their profiles from the platform).[21] 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.[22]

In other cases, websites can 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.

---

[21] 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/

[22] *Id., see also* 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/.

1. Effectiveness

This method offers only a probabilistic age estimate. Its effectiveness depends on a platform's ability to link a user's engagement with the website to previous website visits, contradicting the government's stated interest in regulating speech. § 27000.5 As with other age assurance methods, the probabilistic nature of "first-party signal analysis" ensures that age estimates will be imperfect, mischaracterizing some adults as children and vice versa. Users can also evade this method by disabling cookies and it may not work if, for instance, 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

As currently used, this method relies on large amounts of user data already stored by the platforms. This method therefore opens the door to many risks associated with storing vast amounts of user data or providing data to an age verification vendor, including heightening the risk that a user's personal information could be hacked or used for nefarious purposes.

Even where the social media platforms parse their own user data to verify age, this method creates a one-sided accountability system whereby the social media website must make probabilistic inferences about user data and then must block or restrict access based on the results, inviting error.

C. Uploading a Government-Issued ID

This method requires a website visitor to share a copy of a government-issued ID. First, the website must determine that the visitor is attempting to access from California. Next, it prompts the visitor to upload their government-issued ID and upload it to the website the visitor is attempting to access (or a third-party verification service). 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.

For example, Veriff, an identity verification company, offers an age validation service that relies exclusively on a government-issued ID.[23] According

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

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."[24] Second, "[t]he calculated age is cross-checked to see if it is above your predefined minimum age threshold."[25] Third, "[t]he age validation result is returned and users below your predefined threshold can be automatically declined."[26] Another company, Yoti, offers a similar age verification service that requires visitors to upload a selfie in addition to their government ID in order to cross-reference the two against each other.[27]

1. Effectiveness

This method is effective only if (1) the website accurately identifies every visitor in California, (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.[28]

---

[24] *Id.*
[25] *Id*.
[26] *Id*.
[27] *See e.g.*, Chelsea Jarvie and Karen Renaud, *supra* note 16 at 10.
[28] *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-

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 California.[29]

Second, online age verification by government ID can be circumvented by borrowing, scanning, or purchasing images of the ID of another person older than 18. 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 above, 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 eighteen. "[E]nterprising teens can easily find various tools and instructions online to create a fake scanned image of an ID card."[30] And the extent of analysis that

---

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 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[.]").

[29] 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/; *see also* ITIF *Protecting Children*, *supra* note 28.

[30] ITIF *Protecting Children, supra* note 28.

most commercial online age verification service-providers perform on an uploaded government-issued ID is unclear. 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.[31]

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, and could block these users from accessing covered platforms or relegate misclassified adults to feeds suitable only for children. *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."[32] 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 any photo ID[.]"[33]. Racial and ethnic minorities also

---

[31] *See, e.g.*, Veriff, *supra* note 23.
[32] 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.
[33] *See id.* at 2–3.

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."[34]

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.[35] These populations are not trivial, especially in California. A recent Pew Research Center study found that California is home to 1.8 million undocumented immigrants, likely the most in any single state in the United States.[36] And according to the U.S. Census Bureau, there are over 4 million disabled Californians.[37]

---

[34] *Id.* at 4.

[35] 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.

[36] Marisol Cuellar Mejia, Cesar Alesi Perez, and Hans Johnson, *Immigrants in California*, Public Policy Institute of California, (January 2025), https://www.ppic.org/publication/immigrants-in-california/.

[37] California Department of Housing and Community Development, https://www.hcd.ca.gov/policy-and-research/intersectional-policy-work/people-disabilities#:~:text=According%20the%20U.S.%20Census%20Bureau,million%20Californians%20have%20a%20disability.

2. Security and Privacy Risks

The use of government-issued IDs to verify age introduces significant security and privacy concerns. These technologies require all the identifying information on a government-issued ID to be paired with information about the website the visitor is attempting to access and transmits this data to external 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 California law as a pretense.

Digital copies of government-issued IDs are themselves a valuable asset for thieves, hackers, and hostile foreign governments.[38] When this information is paired with an individual's social media presence—which can reveal a person's close contacts, family relationships, real-time location, sexual orientation, pregnancy status, or reproductive health decisions—such data also becomes a target for crimes such as extortion.[39] Other than the deletion requirement of Section 27001(b), discussed in greater detail below, SB 976 currently establishes no affirmative duty on Operators, age-verifiers, third parties, or intermediaries to

---

[38] *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").

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

secure any information used to verify a visitor's age from accidental disclosure or data breach. Nor does it establish a private right of action for individual users.

D. Third-party Databases and Analysis

Some third-party services assemble databases that allow them to match certain personal identifying information to an estimated age, a method of "age assurance," which is less accurate than age verification. 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.[40]

1. Effectiveness

These methods are both ineffective at ensuring exclusion of children and 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.

[40] Chelsea Jarvie and Karen Renaud, *supra* note 16 at 10.

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 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.[41]

E. Zero-Knowledge Proof Systems

Zero-Knowledge Proof ("ZKP") technology is a cryptographic method of verification that allows one party (the prover) to prove the validity of a statement to another party (the verifier) without revealing any information about the statement itself. In the context of age verification, ZKP would allow individuals to confirm they meet an age threshold, without disclosing their exact date of birth or other personal information.[42]

1. Effectiveness

While ZKP presents an opportunity to verify age without disclosing identifying information at the moment a visitor enters a website, it does not eradicate the need for an initial collection and verification of personal information to create the pre-verified data bank that is then encrypted and used for this verification process. For a ZKP technology to work it needs a robust and trusted system to issue and manage the cryptographic credentials it relies upon to verify (e.g., the DMV could issue digital IDs, encoding individuals' underlying

---

[41] 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.

[42] Jared Ronis, *Don't Trust When You Can Verify: A Primer on Zero-Knowledge Proofs*, Wilson Center, https://www.wilsoncenter.org/article/dont-trust-when-you-can-verify-primer-zero-knowledge-proofs.

information).[43] This process requires significant resources and is a barrier for some uses.[44]

Last year, California made digital IDs available to all residents, but the service is only available to those with a smartphone.[45] As of January 2025, only 1 million Californians had a mobile driver's license.[46] California's digital ID capabilities are still in their infancy and cannot satisfy the purposes of SB 976.

2. Security and Privacy Risks

ZKP's reliance on a database of encrypted personal information presents unique risks. ZKP's reliance on a single point of truth to manage credentials creates a centralized vulnerability, which invites large-scale data breaches.[47] This risk is compounded by the fact that government agencies, the likely owners of cryptographic databases, are ill-equipped to securely encrypt and protect the data that sits behind any ZKP system.[48] While ZKP offers a theoretical solution for age

---

[43] *Id.*
[44] Phillip Shoemaker, *What Are Zero-Knowledge Proofs (ZKP)?* (January 13, 2025), https://www.identity.com/zero-knowledge-proofs/.
[45] Keely Quinlan, *California DMV partners with biometric identity company for mobile driver's license program*, (November 13, 2024), https://statescoop.com/california-dmv-partners-with-biometric-identity-company-for-mobile-drivers-license-program/.
[46] *California DMV invites public to mobile driver's license hackathon public briefing* (January 7, 2025), https://www.dmv.ca.gov/portal/news-and-media/california-dmv-invites-public-to-mobile-drivers-license-hackathon-public-briefing/.
[47] Phillip Shoemaker, *supra* note 44.
[48] Shweta Sharma, *11 times the US government got hacked in 2023* (June 13 2024),

verification, its practical implementation poses significant resource challenges and it ultimately presents similar privacy risks as other verification technologies.

F. 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.[49] While this process typically happens in seconds, it requires transferring sensitive information through multiple host websites.

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, sharing the same information one would for an online purchase. The issuing bank then reviews the cardholder's account and approves or denies the charge and the website uses that information to determine access.

1. Effectiveness

This method is generally ineffective because possession of a credit or debit card does not guarantee that an individual is an adult. Many credit card issuers

---

CSO Online, https://www.csoonline.com/article/2145769/11-times-the-us-government-got-hacked-in-2023.html; Jonathan Grieg, *Hackers accessed more than 19,000 accounts on California state welfare platform* (April 26, 2024), The Record, https://therecord.media/hackers-breached-california-state-welfare.

[49] *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/.

allow the primary account holder to add a child as an authorized user.[50] Moreover, many banks allow minors to have their own debit cards.[51]

This method may also prevent adults from accessing design features they are legally permitted to use. The FDIC reported in 2021 that more than a quarter of U.S. households lacked any credit card.[52]

2. Security and Privacy Risks

This method is also inherently risky. Authorizing a card transaction requires users to go through the same steps they would to complete any online transaction. When used for age verification, this already valuable information is paired with the user's potentially sensitive personal data, amplifying risk.

III. The Ineffectiveness and Security Flaws of Current Age Verification Methods Burden Adults' Access to Constitutionally Protected Speech.

As Appellant explained, the Supreme Court has held that laws imposing content-based burdens on adults' access to constitutionally protected speech are subject to strict scrutiny. Brief of Appellant at 49-50. SB 976 is a content-based restriction because it "single[s] out websites facilitating social interaction" while

---

[50] 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/.

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

[52] F.D.I.C., *2021 FDIC National Survey of Unbanked and Underbanked Households*, 2021 Executive Summary, at 6 (Oct. 2022).

exempting many websites that also use "addictive algorithms" for different purposes, such as "commercial transactions" and "customer reviews." *Id*. The issue of content-based burdens on speech is implicated in *Free Speech Coalition v. Paxton*, currently before the Supreme Court. Regardless of that case's outcome, the limits of technology currently available to satisfy SB 976's age verification requirements (discussed *supra*) will exacerbate the burden to adults' access to protected content without furthering the government's objective of protecting children.

A. Implementing SB 976 With Current Technology Will Necessarily Prevent Some Adults from Accessing Some Protected Content Altogether.

The District Court rejected NetChoice's challenge to SB 976 on the basis that age verification might be achieved by a "process[] that run[s] in the background" and "may not appreciably depress adults' access to speech at all." *Netchoice,* 2024 WL 5264045, at *7. But the court below dramatically underestimated the threat posed by available technologies to an adult user's First Amendment rights. No matter which method(s) an Operator uses, some adults will erroneously be denied meaningful access to the platforms governed by SB 976. Misidentification of an adult as a minor may also restrict the array of content displayed to those adult users to only content suitable for minors. Worse, should platforms decide not to offer alternative versions of their algorithmic feeds that

comply with SB 976, misclassified adults would be treated as minors and lose access to personalized feeds altogether.

B. The Security and Privacy Risks Associated with Current Technologies Also Burden Adults' Access to Protected Content.

All the existing technologies that allow a website to verify a user's age require the use of sensitive personal information. As a result, SB 976 forces adults to take on significant risks to their privacy and anonymity to access protected material, which will chill speech.

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 have already been hacked. As one example, the company AU10TIX, left login credentials exposed online *for over a year*, compromising "millions of users" personal information, including facial images and driver's licenses.[53]

In addition to the risk of a data breach, as discussed above, SB 976 currently lacks necessary safeguards of privacy protection, confidentiality, and legal recourse when things go wrong. These risks are exacerbated by the fact that a user's personally identifying information will be linked to their social media

[53] 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).

account. The sale of personal data disseminated online 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."[54] Cybercriminals have already targeted this kind of information.[55] Even The White House has warned of similar threats.[56]

C. SB 976 Will Also Fail to Achieve its Purpose of Protecting Children.

As noted, many forms of age verification are imprecise. Each method described *supra* 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, biometric-scanning technology, or

---

[54] 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.

[55] *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.

[56] 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/.

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 are easily circumvented, allowing minors to access "addictive feeds" despite SB 976's restrictions. Government-issued ID scans can be bypassed when children alter and falsify IDs.[57] Users can defeat biometric scanning by using deepfakes to bypass video or voice "liveness" checks—technology which is becoming increasingly available.[58] Minors 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.[59] 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.[60]

---

[57] Clare Y. Cho, Cong. Rsch. Serv., R47884, *Identifying Minors Online* (Jan. 2, 2024) at 5, https://crsreports.congress.gov/product/pdf/R/R47884.
[58] 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.
[59] 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/.
[60] 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-

D. SB 976 Lacks the Necessary Safeguards to Satisfy Constitutional Tailoring Requirements or Address Pertinent Risks

For a "regulation of the Internet designed to prevent minors from gaining access to harmful materials" to stand, it must be narrowly tailored. *Ashcroft v. ACLU*, 542 U.S. 656, 672 (2004) (*Ashcroft II*). In the words of Justice Frankfurter, narrowly tailoring government regulation of speech avoids "burn[ing] the house to roast the pig." *Butler v. State of Michigan*, 352 U.S. 380, 383 (1957). For a law like SB 976 that regulates speech pursuant to an expressed government interest to be "narrowly tailored" it would need to (1) accurately verify user age *without* identifying the individual, (2) build in privacy protections and assure confidentiality by law, and (3) provide for a private right of enforcement for violations of privacy. *Ashcroft II*, 542 U.S. at 661. SB 976 fails on all three of these important factors.

1. Age Verification Without Identifying an Individual

Although the prescribed method(s) of age verification required by SB 976 have yet to be decided, nothing in the law narrows the universe of technologies for "reasonably determin[ing]" that a user of a covered platform is a minor (or that an adult is their parent) to those that do not rely on personally identifiable information. As outlined above, however, there are no reliable technologies

---

vpns-for-online-privacy-you-might-be-putting-your-data-at-risk.

currently available to precisely verify a website user's age without using that person's identifying information, such as an image, identification card, transaction, post, or biometric information. Even the age assurance technologies that do not seek to link an age estimate to an identity require the collection and analysis of personal identifiable information, including users' biometric information. This scenario poses serious risks for children and adults, as the requirement to disclose personally identifiable information for access to social media platforms' features will increase privacy violations and consequently chill speech. *See e.g. Ashcroft II*, 542 U.S. at 673; *Reno v. ACLU*, 521 U.S. 844, 882 (1997).

2. Privacy Protections and Confidentiality Must Be Assured by Law

SB 976's restrictions on minors without parental consent introduces two levels of necessary verification data—first, age and second, parental relationship to a minor—that will require all users of covered platforms to submit personally identifiable information to access them and expose themselves to further risk of privacy breach in doing so.

Notwithstanding the limited purpose and deletion requirements outlined in § 2700, SB 976 requires that some identifying information will be stored for annual reporting purposes. More concerningly, these limited purpose and deletion requirements do not clearly apply to third-party age verifiers. These requirements impose no confidentiality requirement, nor does SB 976 offer an independent

mechanism for users to enforce the security of their data. Practically speaking, 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. Even if data is anonymized, SB 976's reporting mandates will require some level of data storage, analysis, and summarization, which further heightens the risk of hacking and misappropriation.

These risks have constitutional implications as they demonstrate the many valid reasons both minors and adults will be deterred from accessing protected speech on social media platforms for fear that their personal data will be left unsecured without any independent means of recourse.

3. Private Rights of Enforcement for Violations of Privacy

Finally, because there are a number of potential opportunities for privacy violations to occur, given the level of personally identifiable information that is required by SB 976, a narrowly tailored restriction would need to provide aggrieved users with a remedy in the event of a breach. *Ashcroft II*, 542 U.S. at 661. SB 976 specifically does not allow for its enforcement unless by civil action brought by the Attorney General. This express exclusion of a private right of action will make recourse for Californians whose privacy is violated as a result of SB 976 virtually non-existent. § 27006(a).

It is also unclear how the Attorney General would monitor every impacted platform and Operator for compliance with these requirements. 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.[61] Thus, the Attorney General will likely only hear about noncompliance with these requirements 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 accurately indicate age without identifying an individual and protect user data and identification.[62] While these technologies are not yet mature, their development suggests it is possible to protect children from harmful material without risking online security and privacy.

However, SB 976 applies heavy restrictions on speech without instituting commensurate safeguards. It does little to protect children from social media addiction and presents significant privacy and security risks that will burden and even prevent adult access to constitutionally protected content.

---

[61] *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.

[62] *See* 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.

DATED: February 6, 2025

/s/ Andrew S. Bruns

Andrew S. Bruns
(California Bar No. 315040)
Flora D. Morgan
(California Bar No. 359733)
Keker, Van Nest & Peters LLP
633 Battery Street
San Francisco, CA 94111-1809
abruns@keker.com
fmorgan@keker.com

Attorneys for Amicus Curiae Center for Democracy & Technology

CERTIFICATE OF COMPLIANCE

I hereby certify as follows:

1. This brief complies with the type-volume limitations of Federal Rule of Appellate Procedure 29(a)(5) and Federal Circuit Rule 29(b). The brief contains 6,968 words according to the word count of the word-processing system used to prepare the brief, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(f) and Federal Circuit Rule 32(b).

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6). The brief has been prepared in a 14-point, proportionally spaced Times New Roman font.

DATED: February 6, 2025

/s/ Andrew S. Bruns
Andrew S. Bruns

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing BRIEF OF AMICUS CURIAE CENTER FOR DEMOCRACY & TECHNOLOGY IN SUPPORT OF PLAINTIFF-APPELLANT with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate ACMS system on February 6, 2025. All participants in the case are registered ACMS users, and service will be accomplished by the appellate ACMS system.

DATED: February 6, 2025

/s/ Andrew S. Bruns
Andrew S. Bruns