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 ATSIGN, INC. AS *AMICUS CURIAE* IN SUPPORT OF PETITIONERS

DEREK T. HO
Counsel of Record
MATTHEW D. READE
KYLE C. BAILEY
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.
1615 M Street, N.W.
Suite 400
Washington, D.C. 20036
(202) 326-7900
(dho@kellogghansen.com)

September 23, 2024

TABLE OF CONTENTS

TABLE OF AUTHORITIES

INTEREST OF *AMICUS CURIAE*[1]

Amicus Atsign, Inc. is a technology company founded in 2019 to fix the problems of data security and identity management online.

Atsign developed the concept of the "atSign"—a unique handle that serves as a person's (or an entity's or thing's) digital identity. An atSign gives you complete control over your data, allowing you to decide what data to share and who can access it. With just an internet connection, Atsign's custom protocol (the atProtocol) enables fast, secure, and encrypted communications between people and entities.

The age-verification systems in use today illustrate a fundamental shortcoming of the Internet that Atsign solves: people have no control over their data online. Texas HB 1181, for example, requires anyone visiting an adult website to expose sensitive, personally identifying data to third parties they may not trust. Those unnecessary disclosures threaten privacy, data security, and autonomy.

A privacy-first age-verification system, such as one powered by Atsign's open-source technology, would allow secure verification without exposing any sensitive data and depriving people of autonomy. Having built its technology on the pillars of data ownership and privacy, Atsign has a powerful interest in promoting this revolutionary (and feasible) alternative to HB 1181.

---

[1] Pursuant to Supreme Court Rule 37.6, counsel for *amicus* represent that they authored this brief in its entirety and that none of the parties or their counsel, nor any other person or entity other than *amicus* or its counsel, made a monetary contribution intended to fund the preparation or submission of this brief.

INTRODUCTION AND SUMMARY OF ARGUMENT

An age-restricted website needs to know just one thing about a person seeking access—whether they are of age. Yet Texas's age-verification policy forces people to expose substantial amounts of unrelated, sensitive personal information to entities they do not trust. For example, uploading a photo of a driver's license to a website reveals far more than a person's date of birth; it also reveals their full name, address, gender, physical attributes, digital signature, and more. And Texas's law denies people any choice over who can have that information. This case is not about adult websites; it is about whether States may require age verification—for any kind of Internet content—in ways that needlessly undermine privacy, data security, and autonomy. The Court should not adopt a legal standard that would permit States to do so.

Over-disclosure and denial of choice have been the status quo on the Internet for decades. As a result, policymakers seeking to enact age-verification laws have accepted the costs to privacy, security, and autonomy as necessary sacrifices—as Texas has done with HB 1181. But there are better approaches. Using well-established technologies, Texas could be the first in the nation to enact a privacy-first age-verification policy that holds people accountable online while preserving their anonymity and autonomy.

Under a privacy-first age-verification system, you, the Internet user, choose whom to trust to verify your age—your bank, the government, your employer, your local library, or your school, to name just a few. Then, you act as an intermediary between that trusted age-verification provider and the age-restricted website you wish to access. By cryptographically transmitting

the verification to the age-restricted website, you can verify your age (or any other attribute) without disclosing any other information. The age-restricted website learns only that your age has been verified, and your trusted age-verification provider never learns why you asked for verification—or to whom you sent that verification.

A privacy-first age-verification system can extend to far more contexts than just accessing pornography, from signing up for a social-media application, to purchasing alcohol, to gambling online.[2] Moreover, the underlying technology is not limited to age verification. Anonymous and accountable access to age-restricted content is just one of countless applications. This privacy-first model can reshape any transaction on the Internet—age-restricted or not—by giving people total control over what data they share and with whom they share it.

Enabling a privacy-first Internet at scale will take time, new policy, and buy-in from key stakeholders. But the technology is here, and Texas should use it. Under long-established First Amendment law, content-based restrictions on speech must satisfy strict scrutiny. *See Ashcroft v. ACLU*, 542 U.S. 656, 665-66 (2004). And people naturally hesitate to turn over personal information to parties they do not trust,

---

[2] Extending age-verification systems to other contexts further protects privacy. If an age-verification system is used only to restrict access to adult content, for example, then age-verification providers (which could include the government) necessarily know that any person asking to verify their age is doing so to access adult content. But if the age-verification system can be used to access a variety of restricted content and for other purposes, age-verification providers cannot infer anything about why the person seeks verification.

especially when it reveals their access to sensitive (but protected) speech. By giving people the choice whom to trust to verify their age, and limiting disclosure of any information besides their age, privacy-first age verification would provide a more effective, less restrictive alternative to Texas HB 1181.

ARGUMENT

I. Privacy-First Age Verification

People constantly have to share data on the Internet. Almost everything done online, from buying lunch, scheduling a vacation, or creating a social-media account, requires you to turn over personal information. Consider how often you sign up for a new app or website and have to fill out the all-too-familiar form asking for your name, phone number, and email address. Your data ends up duplicated, out of date, spread out all over the Internet, and susceptible to hacking.

Age verification on the Internet follows the same pattern. Despite needing to know only whether you are of age, age-verification systems in use today force you to turn over a vast trove of sensitive information. You have no control: to access an age-restricted website, you are forced to expose unnecessary information about yourself to entities you may not trust, hindering your privacy, leaving your data vulnerable, and removing your autonomy.

There is a better solution. Privacy-first age verification can give people, rather than untrusted websites and age-verification providers, control over their data.

At a high level, here is how a privacy-first age-verification system would work:

To create the system, policymakers would first certify a set of verifiers. These age-verification providers

could harness current age-verification methods, such as verifying age through a government-issued ID, credit card, or biometric information. Any trusted entity that knows people's age could serve as a verifier—from a government-run ID service to a bank or your local library. Policymakers can vet and control the available verification methods. But crucially, *people*, not age-restricted websites, make the ultimate choice of which provider they trust to verify their age.

If you try to access an age-restricted website while in Texas, that website would ask you to verify your age. But then, *you* would get to choose which verifier you trust to verify your age. You are not forced to use a verification provider chosen by the age-restricted website. Nor must you disclose any information about yourself to a verifier that does not already have it.[3] And, because you stand between the age-restricted website and the verifier, the verifier cannot learn anything about the site you are trying to access.

The verifier then checks whether you are of age and provides a "yes" or "no" answer, which you pass on to the age-restricted website through an encrypted message. The age-restricted website learns nothing about you except for whether you are of age. You remain completely anonymous.

To further illustrate this privacy-first age-verification system, the following section discusses a potential implementation utilizing Atsign's open-

---

[3] For example, suppose that you choose the government to verify your age. If the government has already issued you an ID, then it already knows your age and who you are. No new personal information must be shared.

source platform, atPlatform, which empowers developers to create privacy-first applications.[4]

A. A Privacy-First Age-Verification System Using Atsign's Platform

The atPlatform flips the Internet's traditional architecture on its head. Instead of websites and applications collecting and storing your data, with the atPlatform, you own and control your data. You create a unique digital identifier, called an atSign, which is akin to a social-media handle, *e.g.*, @amicus. Anyone, including people, entities, and things (like a printer or a smart lamp), can have an atSign.

Each atSign, in turn, has an atServer, which stores the atSign's encrypted data. atServers can be run by anyone on a variety of platforms, including popular cloud services like Amazon Web Services, Google Cloud Platform, Microsoft Azure, and Oracle Cloud Infrastructure. The atServer is accessible over the Internet and easily managed by the owner from their computer, phone, or tablet. With this architecture, your data is stored once and encrypted at rest (*i.e.*, not just when you share or transfer that data). So only you can access your data. The atPlatform enables secure communication between atSigns and allows atSigns to easily prove their authenticity to others. If you choose to share your data, that communication is end-to-end encrypted, surveillance-free, and resistant to attack.[5]

---

[4] *See generally The atPlatform White Paper*, Atsign, https://atsign.com/resources/white-papers/the-platform-white-paper/.

[5] Atsign's technology also allows people to provide different answers to the same question depending on who is asking. For example, if someone asks for your location, you could respond with your exact location based on your phone's GPS, but you may

Having people own their data—rather than countless online companies—creates accountability. Everyone gains responsibility for their data, making it easier to manage and control their information and protect it from misuse. Rather than having to re-input the same personal information over and over on different apps and websites, you just share your atSign and grant the app or website access to the requested information. Updating your information then is easy. Suppose you get a new credit card. You need to update your card information only once, where it is stored in your atServer, and your atServer automatically notifies any entity that you have granted access, such as an online bookstore or your favorite coffee shop's app.

The atPlatform allows for self-sovereign identities, a digital identity model where each person has sole control over the information they use to confirm their identity online.[6] Through their atSigns, everyone has control over who can access their data, what data they can access, and how long they can access it. You can also easily rescind access to your data if you no longer trust an entity you previously gave access.

An age-verification application built on the atPlatform would allow people to be accountable on

---

not be comfortable giving everyone that much detail. Instead of giving the same answer to everyone, you can provide different levels of detail depending on how much you trust who is asking, from responding with the State in which you live, to responding with your postal address, to giving even more contextual responses like that you are "at the office" or "downstairs." Enabling context-aware responses unlocks additional functionality and gives people an extra degree of privacy and control over their information.

[6] *See* Christopher Allen, *The Path to Self-Sovereign Identity*, Life With Alacrity (Apr. 26, 2016), http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

the Internet while remaining anonymous. Consider the following potential implementation:

Texas wants to verify that anyone accessing websites with adult content is at least 18 years old. To do this, the State approves a set of verifiers, including the DMV (@texas_dmv),[7] banks (*e.g.*, @bank), and a third-party attester that offers biometric age verification (@biometric_verifier). Importantly, this set of verifiers could include any entity that knows and can accurately verify a person's age—from banks and utility companies to your local library—giving people a wide variety of options.

An adult in Texas (@texas_adult) tries to access an age-restricted website (@adult_website). @adult_website requires @texas_adult to provide verification that they are at least 18 years old before allowing them to access the website. @texas_adult then can use any of the verifiers approved by Texas to attest that they are of age. Crucially, @texas_adult can decide which verifier they trust. Unlike under Texas HB 1181, @texas_adult is not forced to turn over their identifying information to anyone who does not already have it.

Looking at the options, including validating through @texas_dmv or @biometric_verifier, @texas_adult decides to verify with @bank. After all, @bank already

---

[7] The State of Texas appears to already have the capability to electronically verify identities. In September 2023, for example, Texas announced "the implementation of [a] State-to-State Verification Service," an electronic database allowing Texas "to electronically check with other participating states" to ensure that applicants for driver's licenses in Texas or those other States have their defunct licenses (*e.g.*, from the State they just moved from) invalidated. Texas Dep't of Pub. Safety, *State to State (S2S) Program*, https://www.dps.texas.gov/section/driver-license/state-state-s2s-program (last visited Sept. 17, 2024).

knows @texas_adult, who has had an account there for years. So @bank verifies that @texas_adult is of age and sends @texas_adult a cryptographically signed proof that contains a "yes" or a "no" depending on whether @texas_adult is of age.[8] Here, the signed proof confirms that @texas_adult is at least 18 years old. @texas_adult provides the cryptographically signed proof to @adult_website and is then allowed access.[9]

Importantly, this privacy-first age-verification system can shield the identity of the party that verified the person's age.[10] Thus, @texas_adult can verify their age through @bank without exposing to @adult_website that they frequent that bank. This is accomplished through a technique known as a group signature, which permits any member of a group to anonymously sign a message on behalf of the entire group.[11] Texas could give all approved verifiers this authority. Contrast HB 1181, which requires people to use the age-verification provider chosen by the age-restricted website they are visiting, denying them any

---

[8] Atsign's technology utilizes cryptographic techniques that allow recipients to prove the authenticity of a signed proof.

[9] This signed proof can be paired with a nonce, a number used in cryptographic communications to ensure that each communication is unique, thus preventing the signed proof from being reused. *See Nonce*, Nat'l Inst. of Standards & Tech., https://csrc.nist.gov/glossary/term/nonce.

[10] *See* Olivier Blazy, *Online Age Verification and Privacy Protection: An Impossible Equation?*, Stanford Cyber Pol'y Ctr. (May 7, 2024), https://www.youtube.com/watch?v=OkE5EwuLV9o.

[11] *See generally* David Chaum & Eugène van Heyst, *Group Signatures*, *in* Advances in Cryptology – EUROCRYPT '91: Workshop on the Theory and Application of Cryptographic Techniques, Brighton, UK, April 8-11, 1991 Proceedings (D.W. Davies ed., 1991).

power to choose their verifier or to hide which verifier they use.

This privacy-first age-verification system also would enable policymakers to require multiple layers of attestation, if they wish. For example, the State could require biometric verification to identify the person using the device, in addition to verifying that the person using the device is of age. Under such a system, @texas_adult would request verification from both @bank (to confirm that @texas_adult is of age) and @biometric_verifier (to confirm that the person using the device is actually @texas_adult). Unlike HB 1181, this system would address the concern that minors can access age-restricted websites by using an adult's identification or a fake identification.

Privacy-first age verification also unlocks new ways to reduce the burdens on adults seeking to access age-restricted content. For example, a State could require people to verify their age on a yearly basis (or less). Rather than having to send a picture of your government ID to an ID-verification service, you could obtain from the government (or any other verifier that knows your age, like your bank) a cryptographically signed proof that verifies that you are of age for the next year. Then, each time you try to access an age-restricted site (or any other age-restricted activity, such as buying a bottle of wine), you could provide the State's attestation without having to re-verify your age every time.

Regardless of the precise implementation, @texas_adult's data is maximally protected throughout the verification process. The verifier has no knowledge of what website @texas_adult was trying to access (or even that @texas_adult was trying to access an age-restricted website); all the verifier knows is that @texas_adult requested age verification. The

age-restricted website, in turn, learns only whether @texas_adult is of age.

B. Other Implementations of a Privacy-First Age-Verification System

Reshaping the Internet to be privacy-first will require thoughtful policy, as well as time and investment from industry stakeholders. But the technology to support privacy-first age verification exists today,[12] and there are still other alternative privacy-first age-verification systems that the State could consider.

For example, the State could implement a privacy-first age-verification system at the device level. In a device-based system, people would verify their age when setting up a device. The device then would act as the intermediary, sharing the person's age verification with age-restricted websites without revealing any identifying information.

To further protect people's information and minimize the amount of data shared between parties, a privacy-first age-verification application could also deploy a well-established cryptographic technique known as zero-knowledge proofs. A zero-knowledge proof is a process that enables one party (the prover) to prove to another (the verifier) that a statement is true without revealing anything beyond the fact that the statement is true.[13] Zero-knowledge proofs can be

---

[12] *See* Sarah Forland et al., New America, *Age Verification: The Complicated Effort to Protect Youth Online* 29 (Apr. 2024) (explaining that "it is already technically possible to build an age verification system that assures privacy"), *available at* https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/.

[13] *See* Kenneth A. Bamberger et al., *Verification Dilemmas in Law and the Promise of Zero-Knowledge Proofs*, 37 Berkeley Tech. L.J. 1, 5 (2022). As an illustration, imagine you are playing

used to securely verify any information, including to prove that a person can access age-restricted content.

Since 2023, France's National Commission on Informatics and Liberty has been testing an age-verification system that utilizes zero-knowledge proofs.[14] France's age-verification system uses a gateway operated by France's social security system to mediate between age-restricted websites and approved verifiers.[15] To be sure, France's system has

---

a game of Where's Waldo with a friend. Ever the eagle eye, you spot Waldo immediately, shouting, "I found him!" Your friend does not believe you. You could easily prove you know where Waldo is by pointing to him on the page. But you want your friend to find Waldo themselves. So how do you prove you know where Waldo is without revealing his location?

One way would be to take a piece of paper much larger than the Where's Waldo book and hide the book behind the paper so that your friend does not know the book's placement. Then, you cut a small hole in the paper at Waldo's location and show your friend, allowing them to see Waldo but nothing else. You have now proven that you know where Waldo is without giving away anything else; your friend still has no clue where Waldo is on the page. *See* Jack Murtagh, *Where's Waldo? How to Mathematically Prove You Found Him without Revealing Where He Is*, Scientific American (July 1, 2023), https://www.scientificamerican.com/article/wheres-waldo-how-to-prove-you-found-him-without-revealing-where-he-is/.

[14] *See* Lauren Leffer, *Online Age Verification Laws Could Do More Harm Than Good*, Scientific American (Apr. 16, 2024) ("The system prevents the website from 'seeing' information that could identify a user. Meanwhile the third-party age verifier cannot detect which site a user is visiting."), https://www.scientificamerican.com/article/online-age-verification-laws-privacy/.

[15] *See* Manual G. Pascual, *How age verification to access porn works in France: 'They won't know anything about you, other than that you're an adult'*, El País (May 7, 2024), https://english.elpais.com/technology/2024-05-07/how-age-verification-to-access-porn-works-in-france-they-wont-know-anything-about-you-other-than-that-youre-an-adult.html.

limitations—chiefly that the government, rather than people themselves, mediates between age-restricted websites and the age-verification provider. But France's system still reduces the amount of data shared to confirm a person's age.[16]

Texas can, and should, push for innovative solutions that allow for robust age verification while protecting people's privacy, security, and autonomy. Instead, Texas has gone down the wrong path, implementing a system that robs people of control over their data and requires excessive disclosures to untrusted parties as a condition of accessing protected speech.

II. Privacy-First Age Verification Offers Significant Benefits over Traditional Age-Verification Techniques

A. Privacy-First Age Verification Preserves Privacy by Giving People Control over Their Data

A privacy-first system offers robust age verification while minimizing the exposure of personal information. This solution enhances privacy by giving individuals full ownership and control over their data.

Under Texas HB 1181, in contrast, anyone attempting to access an age-restricted website is forced to expose significant amounts of sensitive personal information to third-party websites just to verify that they are of age. That information can include their full name, address, gender, physical attributes, digital signature, or even biometric information, such as facial geometry. This approach naturally raises

---

[16] *See Adult websites: protecting minors and adults' identities at the same time*, French Inst. for Rsch. in Computer Sci. & Automation (Inria) (updated July 18, 2024), https://www.inria.fr/en/adult-websites-security-privacy-minors-adults.

significant privacy concerns: individuals have no control of their data and are forced to reveal far more than necessary to prove just that they are at least 18 years old.

With privacy-first age verification, individuals have full control over their personally identifying information and are able to limit both what personal information they provide and to whom they provide it. The process is simple and straightforward, with clear privacy benefits. You do not have to expose any personally identifying information, not even your date of birth, to age-restricted websites. Instead, the age-restricted website learns only what it needs to know: whether you are of age.

The system also reduces concerns over government surveillance.[17] Instead of exposing to the government or other verifiers which websites you are accessing, a privacy-first system reveals nothing about why you are verifying your identity. And with sufficient buy-in from industry stakeholders and thoughtful government policy,[18] a privacy-first system can extend to many other contexts requiring verification of age or other aspects of your identity, eliminating any risk that seeking age verification could reveal something about you or what you want to access.

---

[17] *See* Pet. App. 125a ("By verifying information through government identification, the law will allow the government to peer into the most intimate and personal aspects of people's lives. It runs the risk that the state can monitor when an adult views sexually explicit materials and what kind of websites they visit. In effect, the law risks forcing individuals to divulge specific details of their sexuality to the state government to gain access to certain speech.").

[18] For example, the State could cooperate with device manufacturers to enable age verification at the device level or to make platforms like Atsign's broadly available to Texas citizens.

B. Privacy-First Age Verification Enhances Data Security

Reducing over-exposure of personal information not only benefits privacy; it also improves data security. Any collection of personal information is at risk of a data breach, inadvertent disclosure, or other misuse.[19] But given its special sensitivity, the data collected for Texas's age-verification policy—personally identifiable information and data disclosing people's sexual activity and preferences—is particularly ripe for attack.

Under Texas's current law, people have to turn over this sensitive data to each age-restricted website they visit, spreading their data across the Internet. While Texas's law requires age-restricted websites to delete identifying information, people in Texas can only hope that those companies and the verifiers that those companies select will comply. And, as the district court found, the law does not require other intermediaries, which could include web browsers and Internet service providers, to delete this information.[20] By contrast, under a privacy-first age-verification system, no personally identifiable information is transmitted to an age-restricted website, so there is no data at risk.

---

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

[20] *See* Pet. App. 126a ("Moreover, while the commercial entities (e.g., Plaintiffs) are required to delete the data, that is not true for the data in transmission. In short, any intermediary between the commercial websites and the third-party verifiers will not be required to delete the identifying data.").

CONCLUSION

Privacy-first age verification is a more effective, less restrictive solution than the website-based age-verification system enacted by Texas HB 1181.

Respectfully submitted,

DEREK T. HO
Counsel of Record
MATTHEW D. READE
KYLE C. BAILEY
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.
1615 M Street, N.W.
Suite 400
Washington, D.C. 20036
(202) 326-7900
(dho@kellogghansen.com)

September 23, 2024