No. 25A97

IN THE

Supreme Court of the United States

NETCHOICE, LLC
Applicant,

v.

LYNN FITCH,
ATTORNEY GENERAL OF MISSISSIPPI
Respondent.

On Emergency Application to the Honorable Samuel A. Alito, Jr., Associate Justice of the Supreme Court for the United States and Circuit Justice for the Fifth Circuit

BRIEF OF *AMICUS CURIAE* TAXPAYERS PROTECTION ALLIANCE IN SUPPORT OF APPLICANT

ADAM B. BANKS
WHITE & CASE LLP
1221 AVENUE OF THE AMERICAS
NEW YORK, NY 10020

MARK S. DAVIES
Counsel of Record
ZACH WILLIAMS
KUFERE LAING
WHITE & CASE LLP
701 Thirteenth Street NW
Washington, DC 20005
(202) 626-3600
mark.davies@whitecase.com

July 30, 2025

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES AND RULES

MISCELLANEOUS

INTEREST OF AMICUS CURIAE[1]

The Taxpayers Protection Alliance (TPA) is a nonprofit 501(c)(4) educational group with a focus on defending free enterprise and championing reduced taxation and limited government principles. Founded in 2011, TPA furthers its mission through its website, the preparation, and dissemination of articles, analyses, and opinion pieces, and through broadcast television, social media, video, and congressional testimony.

To advance its mission, TPA has participated in cases in front of the Court as *amicus curiae* across a range of issues, including government regulation of electronic tobacco products, *see FDA v. Wages and White Lion Invs., LLC*, 604 U.S. ___, 145 S. Ct. 898, 916 n.3 (2025), and the First Amendment speech and association rights of social media platforms infringed by two state content moderation laws, *see Moody v. NetChoice, LLC*, 603 U.S. 707 (2024).

TPA fights tirelessly for the rights of taxpayers and for consumers struggling to navigate a marketplace made increasingly complex and less free by government interference. Millions of Americans see social media platforms as a revolutionary way to speak their truth, including anonymously if needed. Users' right to use these platforms for anonymous speech is in danger due to Mississippi House Bill 1126 (2024), which threatens to diminish the social media experience for all users.

---

[1] Under Supreme Court Rule 37.6, *amicus* affirms that no counsel for a party authored this brief in whole or in part, and that no person other than *amicus* or its counsel contributed money intended to fund preparing or submitting this brief.

TPA welcomes this opportunity to defend the rights of social media users to free and anonymous speech and protect taxpayers from paying to enforce vaguely written and unconstitutional statutes. TPA submits this brief to detail why mandated social media age verification impermissibly burdens social media users' right to anonymous speech *and* undermines Mississippi's stated interest in protecting minors. *See Ruckelshaus v. Monsanto Co.*, 463 U.S. 1315, 1317 (1983) (Blackmun, J. in chambers) (recognizing that the loss of anonymity is an irreparable harm).

SUMMARY OF ARGUMENT

Mississippi House Bill 1126 ("H.B. 1126," "the Act") unconstitutionally burdens social media users' First Amendment rights by mandating an age verification system that impedes anonymous speech and association. Anonymity in political and social discourse is among the chief "values protected by the First Amendment" and goes "to the very notion of a free society." *Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton*, 536 U.S. 150, 166–67 (2002). Nothing is more offensive to both than a law that demands a citizen to "first inform the government of her desire to speak to her neighbors and then obtain a permit to do so." *Id.* at 167.

H.B. 1126 defies this well-established tradition and this Court's cases that repeatedly protect the right to anonymity in speech and association. Age verification systems require users to upload sensitive documents or biometric data before engaging in speech on social media platforms that have become central avenues for public discourse. In so doing, the Act effectively requires users to link their identities

to their online expression, chilling speech and infringing on the fundamental right to associate privately, even if disclosure is only to private parties or intermediaries.

While the state could satisfy strict scrutiny by demonstrating that age verification is the least restrictive means of furthering a compelling government interest, the law *detracts* from the safety goals set forth by Mississippi. Requiring social media companies to collect such sensitive personal identification data makes them even more vulnerable to cyberattacks, hacking, and data breaches. Many corporations (big and small) and specialized identity-verification services have suffered repeated breaches, demonstrating that even well-resourced entities cannot guarantee user data security. Mississippi's law would expose millions of users to these risks by aggregating vast amounts of sensitive information in a way that both increases the threat of exploitation and deters users from participating in digital platforms.

H.B. 1126 thus not only imposes unconstitutional restrictions on anonymous expression and association but also undermines the very interest it claims to serve—protecting minors—by making digital life more dangerous and less accessible. Only immediate relief from the Court can avoid these dangers and safeguard users' First Amendment rights.

ARGUMENT

I. Allowing House Bill 1126 to Take Full Effect Would Impermissibly Infringe on Social Media Users' First Amendment Right to Anonymity.

Mississippi's House Bill 1126 impermissibly burdens social media platform users' First Amendment rights to anonymity in expression and affiliation. The

regulatory requirements imposed by this legislation will make it immeasurably more difficult for the millions of digital consumers represented by the TPA to speak their minds freely on the websites of their choice.

1. The right to speak anonymously is jealously "protected by the First Amendment" and sits at "the very notion of a free society." *Watchtower Bible & Tract Soc'y of N.Y.*, 536 U.S. at 166. A mandate requiring citizens to "first inform the government of her desire to speak to her neighbors and then obtain a permit to do so" is nothing short of offensive. *Id.* "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind." *Talley v. California*, 362 U.S. 60, 64 (1960). "Great works of literature have frequently been produced by authors writing under assumed names." *McIntyre v. Ohio Elections Comm.*, 514 U.S. 334, 341 (1995). The decision to publish anonymously is deeply personal: "an advocate may believe her ideas will be more persuasive if her readers are unaware of her identity." *Id.* at 342. So, an anonymous publication "provides a way for a writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent." *Id.* And there can be no dispute that anonymous publications have greatly benefitted "the marketplace of ideas." *Id.*; *see also id.* at 341 n.4.

Anonymous publication also furthers political speech. In this context, the decision to speak anonymously may be "motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible." *McIntyre,* 514 U.S. at 341–42. In the political

realm, anonymous publication serves as the vehicle for "[p]ersecuted groups and sects from time to time throughout history … to criticize oppressive practices and laws," *Talley*, 362 U.S. at 64. And speakers who wish to protest government overreach may be presented a Hobson's choice: speak anonymously "or not at all." *Id.* "Thus, even in the field of political rhetoric, where the identity of the speaker is an important component of many attempts to persuade, the most effective advocates have sometimes opted for anonymity." *McIntyre*, 514 U.S. 343 (internal citation and quotation marks omitted).

On this score, we need look no further than our founding. "There is little doubt that the Framers engaged in anonymous political writing." *Id.* at 360 (Thomas, J., concurring). James Madison, John Jay, and Alexander Hamilton, of course, published the Federalist Papers "under pseudonym of 'Publis.'" *Id.* Without their contributions, nationhood may have proven a fleeting concept. Anonymity serves a similar function in modern political discourse: forced identity disclosure "discourages participation" in the democratic process and rarely has "sufficient cause." *Buckley v. American Constitutional Law Found.*, 525 U.S. 182, 200 (1999). Individuals cannot feel completely free to express their views, no matter how fringe or "dangerous" those views are, if their identities are held hostage to compulsory government regulation. Press licensure and forced disclosure were characteristics of the Crown, *not* the free society established under our Constitution.

The First Amendment's protection of anonymity is not limited to speech. This Court has long recognized "the vital relationship between freedom to associate and

privacy in one's associations." *NAACP v. Alabama*, 357 U.S. 449, 462 (1958)." And, because of this inseverable relationship, "[t]he Constitution protects against the compelled disclosure of political associations and beliefs." *Doe v. Reed*, 561 U.S. 186, 232 (2010) (Thomas, J., dissenting); *see also Brown v. Socialist Workers '74 Campaign Comm. (Ohio),* 459 U.S. 87, 91 (1982). When Alabama demanded disclosure of the NAACP's membership rolls as a condition of continued operation in the state, this Court held that "[i]nviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." *NAACP*, 357 U.S. at 462.

This Court has doubled down on its canonical holding in *NAACP v. Alabama*. In *Shelton*, for example, the Court held that disclosure requirements can chill association "[e]ven if there [is] no disclosure to the general public." *Shelton v. Tucker*, 364 U.S. 479, 486 (1960). And just a few terms ago, in *Americans for Prosperity Foundation*, the Court reemphasized its holdings in *NAACP* and *Shelton* when it, again, protected the right to anonymity while emphasizing that the age-old risks of "bomb threats, protests, stalking, and physical violence" are now heightened in the 21st century. *Americans For Prosperity Found. v. Bonta*, 594 U.S. 595, 617 (2021). Today, and "with each passing year," "'anyone with access to a computer can compile a wealth of information about anyone else', including such sensitive details as a person's home address or the school attended by his children." *Id.* (quoting *Reed*, 561 U.S. at 208 (Alito, J., concurring)).

2. Courts have held that internet users, who engage in chatrooms or (as here) explore social media platforms, have the same right to remain anonymous—in this respect, they are no different than their predecessors who distributed handbills. In the early days of the internet, Georgia prohibited internet data transmission "if such data uses any individual name ... to falsely identify the person." *ACLU of Georgia v. Miller*, 977 F. Supp. 1228, 1230 (N.D. Ga. 1997) (quoting Ga. Code § 16-9-93.1). This law was quickly enjoined because "the identity of the speaker is no different from other components of [a] document's contents that the author is free to include or exclude"; identification-related requirements constitute a "presumptively invalid content-based restriction." *Id*. at 1232 (citing *McIntyre*, 514 at 340–42).

Mississippi's demand that covered websites "make commercially reasonable efforts to verify the age of the person creating an account with a level of certainty appropriate to the risks that arise from the information management practices of the" website similarly violates the First Amendment. § 4(1). "The only method that can determine a user's age to a sufficient degree of confidence is to require every user, no matter what age they claim to be, to upload government-issued identification, deanonymizing themselves and jeopardizing their privacy." App.211a. So, it is no surprise that many users respond to requests for government issued identification with intense skepticism due to fear that they are being "scammed." App.199a.

The users' skepticism is well-founded. Requests for government issued identification create "serious data privacy vulnerabilities by requiring social media platforms to collect immense amounts of personal data—whether it be government

identification, or photos and recordings for biometric verification." *NetChoice v. Carr*, 2025 WL 1768621, at *14 (N.D. Ga. June 26, 2025); *see also Reed*, 561 U.S. at 208 (Alito, J., concurring). Making matters worse, under Mississippi's law, social media platforms are forced to *constantly* collect their users' personal biometric data. "Because people can move at any time and can travel to states they don't reside in, a single deanonymization and identity verification at the time of account creation would be insufficient to comply with the Act." App.212a. Compliance requires a data collection system that accounts for the possibility that "people can move at any time and can travel to states they don't reside in," so social media platforms "would need to perform regular deanonymization and identity verification checks of all users." App.212a.

Neither the platforms, nor its users, want to participate in such an intrusive regime. It is no surprise that social media platforms "expect even higher numbers of prospective and current users to decline to join the platform or be unable or unwilling to provide government identification." App.200a. At a minimum, the age-verification requirement creates "an independent chilling effect on [users'] speech and access to information." *Carr*, 2025 WL 1768621, at *14.

What's more, government identification includes "more sensitive piece[s] of information than simply date of birth." App.200a. So even though § 4(1) purports to force social media platforms to collect only a user's age, in reality, Mississippi forces users to disclose their names and address. And users of these platforms include "marginalized people who experience heightened personal security concerns"

including "Russian" and "Chinese" "activists" who publish online speech "protesting their government's human rights abuses." App.213a. These activists are comfortable on these platforms because they "do not cooperate with their government's mandated censorship and do not require them to provide [] personally identifying information that may be discoverable by their government." App. 213a-14a. Section 4(1) is no different from the compelled disclosures in *NAACP*, *McIntyre*, and *Buckley* that violated the First Amendment right to anonymity.

The fact that NetChoice's members have already implemented policies that accomplish H.B. 1126's purported goals underscores § 4(1)'s constitutional defects. *See* App.238a-48a. To the extent that H.B. 1126 reflects the general purpose to protect minors from viewing obscene or harmful content, the organization's members "have put in place important mechanisms to address and—as appropriate—remove nudity and sexual content, self-harm, substance abuse, harassment and bullying, and child exploitation." App.7a. These self-regulated measures do not chill speech—nor do they force users to disclose their identity to the government. Mississippi cannot show that this new layer of regulation—as opposed to existing, private content moderation efforts and an array of federal laws already designed to remove various illicit material from platforms[2]—is a well-tailored approach to the problem of "protecting minor children from online harmful material" stated in the long-form title of H.B. 1126.

---

[2] *See* TAKE IT DOWN Act, Pub. L. No. 119-12, 139 Stat. 55 (2005) (prohibiting online publication of intimate visuals and likenesses of individuals); Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1214 (1996) (criminalizing "material support or resources" to even the nonviolent activities of a designated terrorist organization).

II. "Commercially Reasonable Efforts" to Verify Age Necessarily Undermine the State's Interests by Placing Minors' Personal and Sensitive Data on the Internet.

Far from furthering a compelling government interest under strict scrutiny, age verification undermines Mississippi's stated interest of protecting minors from harmful material online. The Act does so by requiring users to upload sensitive, personal information as the cost of exercising the right to free speech on a social media platform.

One way social media companies can protect users' privacy is through the practice of data minimization and proportionality. This entails collecting only the minimum amount of personal data needed to accomplish a purpose. Platforms are able to implement robust and effective protection measures, including automated and manual content moderation, age requirements, and parental controls, without requiring additional verification measures.

The Act impedes those efforts by requiring social media companies to amass sensitive data on its users. Age verification requires users to submit personal data to prove their age. Verification typically takes the form of an uploaded image of government-issued documentation—such as a birth certificate or driver's license—or a facial scan. Every piece of data uploaded to a platform's system increases its vulnerability to a hack, data breach, or other cyber incident that would compromise the data security and privacy of the user. Indeed, uploading the sensitive data H.B. 1126 requires, to even a single social media platform, risks turning this data into a target for hackers. All of this is data that platforms choose *not* to collect, in part so their systems do not become rich targets for hackers.

That threat is multiplied by the vast number of social media platforms minors join. Approximately 253 million people use social media in the United States, which represents about 73 percent of the population. Most use multiple platforms.[3] According to a 2024 study, 78.3 percent of Mississippians ages 15 and above do so.[4] Teens in the United States interact with an average of 40 apps in a single week, nearly half being social media platforms.[5] H.B. 1126 would require the submission of verification data to each of these platforms, thereby increasing the number of platforms in possession of user data targeted by hackers.

The sheer amount of information aggregated due to mandated age verification would flood the internet with data—intimate, personal data—which would be incredibly attractive to, and the targets of, cybercriminals and other bad actors. As Justice Alito noted during oral arguments in *Free Speech Coalition v. Paxton*, "There have been hacks of everything."[6] According to a Duke University analysis, four-fifths of companies report having fallen victim to hacks.[7] Large corporations such as Target (2013), Equifax (2017), Marriott International (2018), Capital One (2019), MGM

---

[3] Shubham Singh, *How Many People Use Social Media 2025 [Usage Statistics]*, Demandsage (May 17, 2025), https://tinyurl.com/mrxtauja.

[4] *Study reveals which US states have the highest population on social media*, Heath Tech Digital (June 14, 2024), https://tinyurl.com/3fyyn8pf; *Social Media Fact Sheet*, Pew Research Center (Nov. 13, 2024), https://tinyurl.com/54bvrfhj.

[5] University of Michigan, "Study: Average teen received more than 200 app notifications a day," https://tinyurl.com/bdz2y3cm.

[6] Justice Alito, Oral Arguments, *Free Speech Coalition v. Paxton* (Jan. 15, 2025), https://tinyurl.com/38jdpppy.

[7] Duke University, "More Than 80 Percent of Firms Say They Have Been Hacked," https://tinyurl.com/ykdnbnxd.

Resorts (2023), and T-Mobile (2023), have suffered hacks of sensitive personal data.[8] Social media platforms and related apps—entrusted by the authors of H.B. 1126 to lead age verification efforts—have also suffered costly breaches.[9] And just a few days ago, the "Tea" dating-related app reported that thousands of images used to verify users' identities had been breached.[10]

This sample of reported incidents shows that even large companies with robust information technology tools face the risk of a data breach. These dangers are increasing over time, driven by the development of new technologies such as artificial intelligence.[11] The Act would raise the stakes of a data breach by loading repositories targeted by hackers with sensitive age-verification data. In other words, H.B. 1126 will only increase the dangers to users—and therefore the burdens imposed on their free speech—in an increasingly dangerous digital world.

For many social media platforms, the "commercially reasonable" efforts the Act requires to verify a user's age would entail contracting with a third-party verification service. While social media companies labor to ensure the safety of their platforms

---

[8] Venkatesh Sundar, *39 Most Notorious Hacks in History that Fall Under OWASP Top 10*, Indusface (Feb. 19, 2025), https://tinyurl.com/4eywfzes.

[9] Barbara Ortutay, *Tea, an app for women to safely talk about men they date, has been breached, user IDs exposed*, Associated Press (July 25, 2025), https://tinyurl.com/yc42ce8t; Aaron Holmes, *533 million Facebook users' phone numbers and personal data have been leaked online*, Business Insider (Apr. 3, 2021), https://tinyurl.com/387tafbb; Davey Winder, *200 Million X User Records Released — 2.8 Billion Twitter IDs Leaked*, Forbes (Apr. 1, 2025), https://tinyurl.com/5caz8xre.

[10] Dearbail Jordan, *Hackers steal images from women's dating safety app that vets men*, BBC (July 26, 2025), https://tinyurl.com/55aknmsf.

[11] *AI Continues to Reshape Cybersecurity Landscape*, App Security Project (Aug. 7, 2024), https://tinyurl.com/4dmzdrtk.

for minors, smaller platform developers may not have the resources to conduct age verification and would have to rely on these services. And even established platforms with significant numbers of existing users do not currently require a user to submit a date of birth to sign up for an account. These platforms may choose to rely on a third party for verification, rather than develop that capability internally, resulting in the transfer of large numbers of users' data to third-party services.

The reliance on third-party services would further spread age verification data into additional vulnerable data repositories. And these services have suffered cyber events, too. Outabox, which provided facial-recognition services to various in-person businesses, announced a massive cybersecurity breach in 2024 resulting in the piracy of more than one million consumer records.[12] AU10TIX, an identity-verification service used by recognizable platforms like Uber, TikTok, X, and LinkedIn, is another victim of cybercrime.[13] According to reporting on the incident, AU10TIX "verifies the identities of TikTok, Uber, and X users, sometimes by processing photographs of their faces and pictures of their drivers' licenses."[14] This is exactly the kind of data that Mississippian social media users—adults and children alike—would likely be required to submit if H.B. 1126 is enforced.

---

[12] Jordan Pearson, *The Breach of a Face Recognition Firm Reveals a Hidden Danger of Biometrics*, Wired (May 2, 2024), https://tinyurl.com/ed3ydz4u.
[13] *'But Third-Party Verification Services Are Secure,' They Said.*, App Security Project (July 12, 2024), https://tinyurl.com/msejsxxd.
[14] Joseph Cox, *ID Verification Service for TikTok, Uber, X Exposed Driver Licenses*, 404 Media (June 26, 2024), https://tinyurl.com/46w97ads.

Many users understand these risks and avoid incurring them. Efforts by platforms such as NextDoor to ask for voluntary submission of date-of-birth verification have resulted in users choosing to close out their accounts rather than provide government-issued ID or even simply report their date of birth. Eric Goldman, a law professor at Santa Clara University and tech-policy expert, describes this behavior as a "U-turn" taken by users reluctant to submit sensitive, personal information as a condition of platform authorization, who choose to leave the platform instead of making "unwanted disclosures."[15] These users, who are concerned about privacy and value anonymous speech, will turn away from social media platforms rather than turn over their personal data. If these users are forced into the choice imposed by the Act—either place sensitive, personal information on the internet, or forfeit their right to speak on the social media platform—they will choose to protect their sensitive information. The Act will have deprived these citizens of their right to free speech on a chosen social media platform. No Mississippian should have to choose between exercising the right to free speech and protecting personal data.

It is tempting to think that technological advances have mitigated or removed the dangers associated with age verification—and therefore can be successfully deployed to further the state's goal of bolstering online safety for children. But forcing users to interact with multiple websites hosting aggregated information and vulnerable to cybercrime *undermines* Mississippi's stated interests, while

---

[15] Eric Goldman, *The "Segregate-and-Suppress" Approach to Regulating Child Safety Online*, 28 STANFORD TECHNOLOGY L. REV. 173 (July 6, 2025), https://tinyurl.com/4zxse24h.

simultaneously diminishing users' ability to speak freely on social media. H.B.1126 therefore cannot survive strict scrutiny.

CONCLUSION

The Emergency Application should be granted.

Respectfully submitted,

/s/ *Mark S. Davies*
MARK S. DAVIES
Counsel of Record
ZACH WILLIAMS
KUFERE LAING
WHITE & CASE LLP
701 Thirteenth Street NW
Washington, DC 20005
(202) 626-3600
mark.davies@whitecase.com

Counsel for Amicus Curiae

ADAM B. BANKS
WHITE & CASE LLP
1221 AVENUE OF THE AMERICAS
NEW YORK, NY 10020

July 30, 2025