

In the
Supreme Court of the United States

NETCHOICE,

Applicant,

v.

LYNN FITCH, Attorney General of Mississippi,

Respondent.

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

**BRIEF OF STOP CHILD PREDATORS AS *AMICUS CURIAE*
IN SUPPORT OF EMERGENCY APPLICATION**

Joshua N. Mitchell
Counsel of Record
Jeremy M. Bylund
John B. Goerlich
WILLKIE FARR & GALLAGHER LLP
1875 K Street Northwest
Washington, DC 20006
(202) 303-1000
jmittchell@willkie.com

Counsel for Amicus Curiae

July 28, 2025

TABLE OF CONTENTS

| | |
|---|----|
| TABLE OF AUTHORITIES | ii |
| INTRODUCTION AND INTEREST OF <i>AMICUS CURIAE</i> | 1 |
| SUMMARY OF THE ARGUMENT | 3 |
| ARGUMENT | 4 |
| I. HB1126 makes no provision for law enforcement..... | 6 |
| II. Age-verification and parental-consent requirements do not make children safer. | 7 |
| III. Age-verification and parental-consent requirements increase the risk posed to children by data breaches. | 10 |
| IV. Unconstitutional laws do not further the protection of children. | 11 |
| CONCLUSION..... | 13 |

TABLE OF AUTHORITIES

Cases

| | |
|--|----|
| <i>Ams. for Prosperity Found. v. Bonta</i> , 594 U.S. 595 (2021) | 4 |
| <i>FEC v. Cruz</i> , 596 U.S. 289 (2022) | 5 |
| <i>Free Speech Coal., Inc. v. Paxton</i> , 145 S. Ct. 2291 (2025) | 4 |
| <i>Packingham v. North Carolina</i> , 582 U.S. 98 (2017) | 4 |
| <i>Trump v. CASA, Inc.</i> , 606 U.S. —, 145 S. Ct. 2540 (2025) | 12 |

Statutes

| | |
|--|--------------------------|
| 18 U.S.C. § 2258A | 2, 9 |
| H.B. 1126 (Miss. 2024) | 3, 4, 5, 6, 7, 8, 10, 11 |
| H.B. 1877 (Fla. 2005) | 1 |
| La. Stat. Ann. § 51:1751 | 8 |
| PROTECT Act, Pub. L. 110–401, 122 Stat. 4229 (2008) | 2 |

Other Authorities

| | |
|---|----|
| Elyse Wyatt, Note, “Manipulating Parents, Exploiting Children: the Need for Government Oversight of Private Youth Facilities,” 33 B.U. PUB. INT. L.J. 103 (Winter 2024) | 8 |
| Ionut Arghire, “900k Impacted by Data Breach at Mississippi Healthcare Provider,” SECURITYWEEK (May 15, 2024), https://tinyurl.com/3443mapy | 10 |
| Jonathan Grieg, “Mississippi electric utility warns 20,000 residents of data breach,” THE RECORD (Feb. 3, 2025), https://tinyurl.com/mr37hua6 | 10 |
| Nat’l Ctr. for Missing & Exploited Child., “2024 CyberTipline Reports by Electronic Service Providers (ESPs)” (2025), https://tinyurl.com/454mztdy | 2 |

| | |
|---|----|
| Steve Weisman, “The Unknown Danger of Child Identity Theft,” FORBES (Sept. 13, 2024), https://tinyurl.com/5724sp39 | 10 |
|---|----|

INTRODUCTION AND INTEREST OF *AMICUS CURIAE*¹

Amicus Stop Child Predators (“SCP”) is a national nonprofit organization that exists for a single purpose: to make children safer. To that end, it works with parents, lawmakers, and policy experts in all fifty states to better educate families, schools, and lawmakers about the potential risks children face both in the real world and online. The most acute of those risks include grooming, luring, and child pornography, though SCP also combats bullying and other harms to children. For nearly two decades, SCP has worked to open lines of dialogue with lawmakers and technology-company stakeholders, seeking to help develop practical solutions to protect children from those risks. Its staff includes an array of experts in government reform, children’s advocacy, and child welfare, and it has achieved significant legislative successes, including spearheading the passage of Jessica’s Law in forty-six states.²

SCP focuses substantial policy efforts on keeping social media—and the Internet more broadly—safe for children. This focus springs from a recognition that online child predation often translates directly to real-world harm—that, for example, child predators use social media and other Internet tools to recruit child sex-

¹ Pursuant to Supreme Court Rule 37.6, *amicus curiae* states that no counsel for any party authored this brief in whole or in part and that no entity or person, aside from *amicus curiae*, its members, and its counsel, made any monetary contribution toward the preparation or submission of this brief.

² Jessica’s Law—originally, the “Jessica Lunsford Act,” H.B. 1877 (Fla. 2005)—is a law requiring that sexual predators convicted of molesting a person under the age of twelve serve a mandatory minimum sentence of twenty-five years in prison and undergo lifetime electronic monitoring, designed to safeguard children from the risk of recidivist predators.

trafficking victims and to groom children for sexual exploitation. Those real-world dangers require a real-world response, and so SCP’s policy efforts also focus on ensuring that law enforcement is appropriately funded and coordinates its efforts both with other relevant law-enforcement agencies and with parents and private-sector actors.

In this connection, SCP operates from the fundamental premise that children are safer when the public and private sectors cooperate on developing and implementing effective child-protection policies instead of engaging in counterproductive finger-pointing. Caring parents are the first line of defense in protecting children online, but the private sector—including NetChoice’s members—plays a critical role in limiting the proliferation of harmful content. Child sexual-abuse material (CSAM) is prolific and traverses all corners of the Internet. Social-media services are mandatory CSAM reporters. *See* 18 U.S.C. § 2258A. In 2024 alone, leading social-media platforms accurately and proactively identified and reported more than *sixty million* photos and videos of children being sexually abused. The volume of these reports—more than 99% of the reports to the National Center for Missing and Exploited Children’s CyberTipline³—reflects social media platforms’ unique qualification and positioning for this difficult but essential work.⁴

The Internet and social media are tools that, in addition to ready access to a

³ Nat’l Ctr. for Missing & Exploited Child., “2024 CyberTipline Reports by Electronic Service Providers (ESPs)” (2025), <https://tinyurl.com/454mztdy>.

⁴ Indeed, in enacting the PROTECT Act, Congress recognized that social media services necessarily play a key role in any comprehensive national strategy for combating child predation. *See generally* Pub. L. 110–401, 122 Stat. 4229 (2008).

wealth of knowledge, provide incalculable social and interactive value for young people—especially those who are disabled, suffer from anxiety, or are in other circumstances that make it difficult for them to connect in person. SCP accordingly works with leading online platforms—including NetChoice’s members—to develop and enforce policies that prioritize children’s safety while still promoting free speech and ensuring children have access to the benefits of this valuable technology. Meanwhile, SCP seeks to ensure that, when government intervenes, it focuses those interventions on enacting effective solutions.

Given SCP’s mission and expertise, SCP would be among the first to support an *effective* bill making Mississippi’s children safer. Unfortunately, Mississippi’s House Bill 1126 (“HB1126”)—regardless of the intentions with which it was enacted—will not further that end. NetChoice’s Application ably explains the fundamental constitutional problems with the HB1126’s overbroad and scattershot attacks on protected speech. SCP writes to highlight Mississippi’s failure to match law to policy goals—an utter dereliction of the Legislature’s duty to tailor that means that, no matter which level of elevated scrutiny governs review of HB1126’s restrictions on speech, HB1126 cannot withstand it.

SUMMARY OF THE ARGUMENT

HB1126 is not tailored to its purpose. *First*, it fails to make any provision for bolstering law enforcement—the only reasonable and lawful means of preventing child predators from continuing their predation. *Second*, HB1126’s parental-consent and age-verification requirements do not further the important role played by caring parents in preventing online child abuse, but instead affirmatively suggest that role

should be limited to a single intervention at the creation of a social-media account. *Third*, the data-collation requirements of HB1126 *affirmatively increase* the danger posed to children by pervasive and inevitable data breaches.

Instead of seeking a sustained and sustainable legislative solution, Mississippi has chosen an approach that does nothing to make children safer. HB1126 represents a violation of NetChoice’s members’ constitutional rights, as well as those of children and parents across the state of Mississippi. Passing HB1126 has already diverted resources that would have been better invested in proactive solutions into dead-end litigation. This Court’s emergency intervention is warranted, and the Fifth Circuit’s stay should be vacated.

ARGUMENT

As NetChoice explains, HB1126 significantly burdens protected speech for NetChoice’s members and Mississippi citizens in a misdirected effort to protect children. *See* Appl. 18–37. Because it burdens protected speech activities based on the content of that speech, the Act is subject to strict scrutiny and must therefore be the least restrictive means of achieving a compelling state interest. *Ams. for Prosperity Found. v. Bonta*, 594 U.S. 595, 607 (2021); *see* Appl. 18. But even if strict scrutiny did not apply, Mississippi’s restriction of “access” to NetChoice’s members’ services triggers intermediate scrutiny. *Packingham v. North Carolina*, 582 U.S. 98, 105–06 (2017); *see Free Speech Coal., Inc. v. Paxton*, 145 S. Ct. 2291, 2309 (2025). Under that more lenient but still demanding standard, Mississippi would need to show that HB1126 is “narrowly tailored to serve a significant government interest.” *Packingham*, 582 U.S. at 105–06 (internal quotation marks omitted); *see FEC v. Cruz*,

596 U.S. 289, 305 (2022) (burden of proving the constitutionality of a challenged restriction of speech rests on the government).

HB1126 fails any level of elevated scrutiny because its provisions simply are not fitted to the purpose of keeping children safe online or in the real world. Most fundamentally, the Act contains *no* funding for or other investment in law enforcement—and so it does not take even one predator out of circulation. As NetChoice explains, Mississippi could have chosen to bolster enforcement of its “existing criminal laws.” Appl. 34; *see* Appl. App’x 155a–56a (identifying relevant Mississippi criminal statutes). By ignoring law enforcement—an essential element in any effective fight against child exploitation—the Act does nothing to combat abuse or to find and punish abusers.

HB1126’s parental-consent and age-verification provisions are ineffective in themselves, giving the impression that parents’ responsibility ends with signing off on their children’s creation of a social-media account. But sustained attention from caring parents remains the first and best line of defense against child predation. Further, not only are those provisions ineffective, they also increase the danger posed to children by data breaches.

SCP has spent two decades fighting for effective solutions to the problem of child predation. Those solutions require lasting legislative and political will, not stopgap feel-good measures, and *especially* not when such measures themselves intrude on children’s fundamental rights and will do nothing but attract litigation and waste states’ resources. Whatever good intentions the Mississippi legislature

began with, HB1126 as passed will instead result in serious negative outcomes for children if it is allowed to enter into force.

I. HB1126 makes no provision for law enforcement.

HB1126 imposes technical and administrative methods of access control and then foists the responsibility for compliance and all its associated costs on the private sector. But the Act's narrow and blinkered approach does nothing—*literally nothing at all*—to reduce the population of predators online. *See* Appl. 34 & Appl. App'x 155a–56a. To the contrary, by purporting to offer a paperwork solution to a real-world problem, Mississippi has both obscured the need to invest more aggressively in robust and well-coordinated law-enforcement responses and camouflaged the State's own failure to do so.

SCP's experience and expertise have taught that government's primary focus in keeping the Internet safe for children should be on bolstering law enforcement to remove predatory criminals from the equation. The online threat environment is pervaded by international criminal enterprises that have access to increasingly sophisticated methods (including so-called “artificial intelligence” large language models that can automate the development of malicious software) for (1) evading security protocols online; (2) locating and targeting vulnerable individuals, including children; and (3) repeatedly propagating CSAM in a manner that makes it difficult to eradicate.

Expecting social-media services to be the primary line of defense against such organized crime—as laws like HB1126 contemplate, *see* HB1126 § 6—is both unrealistic and counterproductive. Private companies cannot arrest criminals. Only

appropriately funded law enforcement can do that. Nor can the threats facing children online be addressed by villainizing government's most important partners in this fight—the social-media services themselves, which are the one reliable pool of CSAM reporters on which law enforcement can rely.

Shoddy social science, sensationalist headlines, and perceived political expediency can yield bad and even dangerous legislation, passed as a quick tire-patch on pervasive problems. It is this Court's responsibility to ensure that the worst of that government overreach is rapidly rebuked. Reducing online predation of children requires more than tangling government's private-sector partners in one more layer of red tape. What is needed the deliberate and dispassionate collection of evidence, followed by that evidence's deployment in arrests and prosecutions to enforce the criminal laws, all pursued in accordance with applicable constitutional restrictions. Anything less will neither remove child predators from circulation nor ensure that, once arrested, they do not swiftly return to the streets. HB1126 does nothing to advance those goals.

II. Age-verification and parental-consent requirements do not make children safer.

HB1126 requires up-front age verification whose ostensible purpose is to identify minors, but that of course burdens the speech of both minors and adults. *See* HB1126 § 4(1). The law then demands the consent of a “parent or guardian” to allow a “known minor” to make a social-media account. HB1126 § 4(2). Unlike more thoughtfully crafted but similarly unconstitutional laws, HB1126 does not even carve out exemptions for emancipated minors or other children who lack nurturing and

supportive parents or caregivers.⁵ *Cf.*, e.g., La. Stat. Ann. § 51:1751(9) (exempting from the definition of “minor” individuals “emancipated or married”). HB1126’s one-size-fits-all demand for parental consent thus effectively cuts out a population that may need the interaction of social media the most.

To be sure, SCP believes strongly that caring parents are—and should be—the first line of defense against online predation, which is why it focuses much of its work on educating parents. There will of course be unfortunate circumstances when government child-protection agencies must step in because parents or guardians can’t or won’t. And where government actors fail, the social media services themselves engage in CSAM reporting and can offer lifelines for children in dangerous situations who lack other means of seeking help. For example, young people trapped in abusive congregate-care settings have turned to social media to report that abuse.⁶ But government child-protection agencies and private industry are at best imperfect backstops to parental responsibility, not a replacement for it.

Unfortunately, the age-verification and parental-consent requirements in HB1126 do not foster parental responsibility. To the contrary, they give the State’s imprimatur to the dangerous notion that a parent’s duty begins and ends at their

⁵ SCP does not suggest that such carveouts would rescue HB1126 from unconstitutionality—only that they would reflect a modicum of additional consideration of the law’s real-world consequences.

⁶ *See generally* Elyse Wyatt, Note, “Manipulating Parents, Exploiting Children: the Need for Government Oversight of Private Youth Facilities,” 33 B.U. PUB. INT. L.J. 103, 111 (Winter 2024) (identifying instances of “[s]ocial media ... provid[ing] a powerful platform for survivors of the Troubled Teen Industry to finally have an effective way to speak out.”).

child’s creation of a social-media account. *See* HB1126 § 4(1) (requiring age verification “to create an account”) & § 4(2) (requiring “consent from a parent or guardian” for a “known minor to be an account holder”). The monitoring-and-censorship provisions in Section 6 of HB1126 further confirm that impression, placing on the service providers themselves the primary duty to police the content minors see. HB1126 § 6(1) (imposing on “digital service provider[s]” a duty to “develop and implement a strategy to prevent or mitigate [a] known minor’s exposure to harmful material and other content”). And completing that misguided picture, the parent may then sue a service provider that fails to sufficiently fulfill that duty.⁷ *Id.* § 7(2)(a)–(b). All this sends precisely the wrong message to Mississippi’s parents—suggesting that they need not offer ongoing guidance or encourage their children to ask about troubling interactions online, because, in Mississippi’s view, the social-media services are themselves responsible for any bad actors using the services.

To be sure, service providers have a duty to report and quarantine CSAM—a duty they fulfill every day.⁸ But by abdicating its own role in sufficiently funding and coordinating law-enforcement efforts, and placing itself and parents in an invented dispute on the side opposite the service providers, Mississippi has chosen a path of unnecessary discord over productive cooperation.

⁷ As NetChoice explains, its members recognize the important role caring parents play in ensuring their children’s online safety, which is why their online services provide suites of tools that allow parents to engage actively in ongoing oversight of their children’s social-media activities. Appl. 7 & Appl. App’x 170a–77a, 237a.

⁸ 18 U.S.C. § 2258A(h)(3); *see supra* fn. 3.

III. Age-verification and parental-consent requirements increase the risk posed to children by data breaches.

HB1126 mandates that companies “make commercially reasonable efforts” to verify users’ age and provides several options through which companies may obtain “express consent from a parent or guardian” for a “known minor” to become an account holder. HB1126 § 4(1), (2). But despite the seemingly diverse options for *collecting* this personally identifying information, once collected and employed for its single-use purpose, the data offers little more than an inviting target for hackers and a correspondingly significant security risk to children.

Indeed, given the realities of data security and the wide swath of “digital service provider[s]” Mississippi seeks to regulate with HB1126, it is less accurate to call this a *risk* than to state that one or more datasets created in response to HB1126 *will inevitably* be breached, exposing children’s personal information to anyone with a Bitcoin wallet and a damaged moral compass.⁹ Children already represent a prime target for identity thieves, who know that breaches of minors’ data may go unnoticed for years—even for a decade or longer—until the children reach adulthood and apply for a student loan or their first apartment.¹⁰ By then, of course, any vestiges of the original criminal act, stored in transitory media on an ever-evolving Internet, will be too long gone for investigation.

⁹ See, e.g., Jonathan Grieg, “Mississippi electric utility warns 20,000 residents of data breach,” THE RECORD (Feb. 3, 2025), <https://tinyurl.com/mr37hua6>; Ionut Arghire, “900k Impacted by Data Breach at Mississippi Healthcare Provider,” SECURITYWEEK (May 15, 2024), <https://tinyurl.com/3443mapy>.

¹⁰ See Steve Weisman, “The Unknown Danger of Child Identity Theft,” FORBES (Sept. 13, 2024), <https://tinyurl.com/5724sp39>.

By demanding the collection and collation of sensitive information, HB1126 exacerbates this already-serious problem. Indeed, because enforcing this misguided law will undoubtedly require Mississippi to obtain and store its own copies of at least some of this trove—for example through litigation-adjacent investigation or kept in the virtual evidence lockers of the courts themselves—HB1126 multiplies the targets for data thieves.

IV. Unconstitutional laws do not further the protection of children.

Protecting children is not a box-checking exercise. Because child predation is an evolving threat, battling it requires a sustained effort from parents, lawmakers, and the private sector. While it may be satisfying for policymakers to pass laws that *purport* to protect children, the wrong laws are worse than pointless—they are actively harmful. Lawmakers who pass a misguided or ineffectual law may nevertheless believe they have fully addressed the problem and move on to other matters, not returning to the issue they believe they have “solved.” And so a law like HB1126 that gives a false impression of fostering child safety may in fact set back effective efforts by years or even decades.

Laws like HB1126 result from the flawed calculation that fundamental constitutional rights can and should be significantly curtailed if doing so gives the impression of a step toward solving a difficult societal problem. Here, as discussed above, that impression is a false one. HB1126’s curtailment of children’s fundamental free-speech rights in aid of an entirely illusory policy fix is, to be blunt, simply indefensible.

Passing unconstitutional laws, moreover, invites litigation. *Even if* it were true

that the Act furthered the protection of children, the overwhelming likelihood is that a law seized with such grave free-speech problems will be held unconstitutional and its enforcement enjoined. Meanwhile, the State will have devoted to litigation much-needed resources that could be better used in enacting *effective* protections, such as funding law-enforcement efforts and prosecuting criminals.

A member of this Court recently reassured the public that the Court’s emergency docket will provide parties affected by federal government overreach with a prompt and effective response to that overreach. *Trump v. CASA, Inc.*, 606 U.S. —, 145 S. Ct. 2540, 2570 (2025) (Kavanaugh, J., concurring) (“When a stay or injunction application arrives here, this Court should not and cannot hide in the tall grass. When we receive such an application, we must grant or deny. And when we do—that is, when this Court makes a decision on the interim legal status of a major new federal statute or executive action—that decision will often constitute a form of precedent (*de jure* or *de facto*) that provides guidance throughout the United States during the years-long interim period until a final decision on the merits.”) (footnote omitted). Having given that assurance and reiterated its role as the swift and final arbiter of constitutional questions affecting millions of citizens, the Court may similarly not “hide in the tall grass,” *id.*, when a State flouts settled constitutional law as Mississippi has done here, lest the “form of precedent” suggested by the Court’s emergency-docket inaction or, worse, by the denial of interim relief improperly signals to courts around the country a change in this Court’s view of that settled law.

Mississippi has enacted into law a blatantly unconstitutional swipe at

fundamental free-speech rights. As explained above, that law will fix nothing but will actually exacerbate real dangers faced by children. The emergency relief NetChoice requests is warranted.

CONCLUSION

For the foregoing reasons and those in NetChoice's application, NetChoice's request for emergency relief should be granted, and the Fifth Circuit's stay order vacated.

Respectfully submitted,

/s/ Joshua N. Mitchell

Joshua N. Mitchell

Counsel of Record

Jeremy M. Bylund

John B. Goerlich

WILLKIE FARR & GALLAGHER LLP

1875 K Street Northwest

Washington, DC 20006

(202) 303-1000

jmittchell@willkie.com

Counsel for Amicus Curiae

July 28, 2025