NetChoice
1401 K Street NW, Ste 502
Washington, DC 20005

NetChoice
Defending Free Speech and Free Enterprise Online

New Jersey S. 4215 | **Constitutional Problems**

New Jersey's Age Verification Bill

Government-imposed age verification requirements are unconstitutional

Government-imposed age verification requirements to access speech are an unconstitutional restraint on the listener and the speaker's First Amendment rights. It prohibits a willing listener from engaging with constitutionally protected speech.

Both age verification and parental consent requirements to access lawful speech have been struck down by the Supreme Court. *Reno v. ACLU*, 521 U.S. 844 (1997) (invalidating age verification requirements to access lawful online speech); *Brown v. Entertainment Merchants Association*, 564 U.S. 786, 795 n.3 (2011) (invalidating parental consent requirements for minors purchasing video games, noting that the law does not enforce parental authority but imposes government authority subject to a parental veto).

This year, the Supreme Court reaffirmed that online speech receives the same level of protection as any other. *303 Creative v. Elenis*, 143 S.Ct. 2298 (2023).

Same Failures in Other States as New Jersey S. 4225

At the same time, multiple states have passed age verification laws for the internet. Notably, Arkansas and Utah passed laws which mirror provisions in SB 4215. NetChoice has sued to enjoin both laws.

In Arkansas, NetChoice secured a preliminary injunction against Act 689. Like this bill, Act 689 would require age verification to ensure that no account holder opened an account without parental permission if the user was under 18. The court struck the law down finding that it unconstitutionally restricted access to lawful speech without narrow tailoring to harmful and unlawful speech. Indeed, such blanket restrictions on access to lawful speech could not withstand even intermediate scrutiny.

The proposed restrictions in S. 4215 are even less constitutional than the Arkansas law. Arkansas merely sought to restrict access and require parental consent for *new* users (which, as we have seen, is unconstitutional), but S. 4215 would impose these roadblocks for new *and existing* users meaning it would cut off access to speech to anyone unable (or unwilling) to verify that he is an adult.

Indeed, this broad language makes the New Jersey proposal more akin to Utah's social media law which NetChoice has sued to enjoin. Utah's law, like the New Jersey proposal, applies broadly to all social media companies with five million users and imposes the same age verification and parental consent restrictions presented in Arkansas's Act 689.

Laws that require age verification and parental consent also pose additional burdens:

1. These laws would put an end to anonymous or pseudonymous speech on social media despite the fact that the ability to speak anonymously is protected under the First Amendment. *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995).
2. By requiring social media companies to collect personal information about their users, it poses a greater risk that the data will be obtained by bad actors. As data breeches become more common, and as users become increasingly privacy conscious, being forced to turn over sensitive data to access speech will chill the user's willingness to provide the information and, therefore, preclude them from accessing and contributing to, lawful speech and discussion.

Outline showing overlap between NJ Bill and UT Complaint

1. "Social media company" means a person that provides or operates a social media platform with at least five million account holders worldwide.[1]
2. A. A social media company shall not permit a New Jersey resident who is a minor to be an account holder on the social media company's social media platform unless the minor has obtained the express consent of a parent or guardian.[2]

---

[1] 8. At the outset, the entire Act violates the First Amendment and the Due ProcessClause because it depends on a vague and content-, speaker-, and viewpoint-based definition of a regulated "social media company." § 13-63-101(9). Through a series of vague definitions and exceptions with arbitrary thresholds, the Act singles out some Internet websites for regulatory burdens based on, among other things, the content they disseminate. The same speech may be heavily regulated—or not regulated at all—based on who is speaking, what is being said, and what website it is being said on. For instance, YouTube must comply with the Act's burdensome requirements. But Netflix is exempted, under at least three exceptions: (1) as a "streaming service"; (2) as a service "where the predominant or exclusive function is . . . entertainment"; and (3) as a service that does not allow users to "upload posts." § 13-63-101(10)(a)(ii), (b)(i)(C), (b)(i)(D). As another example, X (formerly known as Twitter), Bluesky, Gab, and Truth Social all allow users to discuss the issues of the day and share similar content. But while X must comply with the Act, Bluesky, Gab, and Truth Social are exempted under the law's arbitrary 5-million account threshold. § 13-63-101(9)(a). Nextdoor appears to be covered by the Act, but if it restricted its community's discussions to "public safety," it would not be. § 13-63-101(10)(b)(i)(I). Minors must secure parental consent (and adults and minors would need to verify their ages) to engage in "interactive gaming" on Facebook, but not on websites like Roblox "where the predominant or exclusive function is . . . interactive gaming." § 13-63-101(10)(b)(i)(F). Anyone searching for a new job on a covered website must jump through similar age-verification hurdles (and minors must secure parental consent), but not on websites providing "career development opportunities." § 13-63-101(10)(b)(i)(J). These are just some of the nonsensical consequences of the Act's multiple content-, speaker-, and viewpoint-based distinctions. Those distinctions all give rise to strict scrutiny, which the Act cannot satisfy. That alone is a sufficient basis to enjoin Defendants from enforcing the Act.

95. The Act's central coverage definition is speaker-based because it does not apply to websites with fewer than "5,000,000 account holders worldwide." § 13-63-101(9). The Act regulates large websites (e.g., X) while ignoring similar expression on similar, smaller websites (e.g., Bluesky, which has about 1.8 million account holders, https://perma.cc/6RYQ-PMLQ, or Truth Social, reported to have about 607,000 monthly users, https://perma.cc/S5SL-B86E).

[2] 9. Moreover, individual provisions of the Act are independently unlawful.

10. *First*, the Act's requirements that covered websites verify the ages of all Utah account holders (both minors and adults) and secure parental consent before allowing minors to create or continue accessing accounts, § 13-63-102, violate the First Amendment. *Griffin*, 2023 WL5660155, at *21 (rejecting similar requirements). The requirements mandate that people of all ages hand over personal information or identification that they may be unwilling or unable to provide. As the Supreme Court has recognized, such requirements burden the exercise of speech and thus violate the First Amendment. *See, e.g.*, *Ashcroft*, 542 U.S. at 673; *Reno*, 521 U.S. at 882. Likewise, the Supreme Court has held that governments may not require minors to secure parental consent before accessing protected speech. *Brown*, 564 U.S. at 799.

62. *Age verification and identify verification.* The Act provides that a "social media company shall verify the age of an existing or new Utah account holder." § 13-63-102(3)(a). "If a Utah account holder fails to meet the verification requirements . . . , the social media company shall deny access to the account." § 13-63-102(3)(b). The Act therefore requires covered websites to verify every account holder's age—including adults—as a precondition to those account holders' access to members' websites. Yet many people may not wish to provide proof of age to gain access to the covered websites. Some people cannot do so.

63. The Act delegates authority to the Division to establish the proper "processes or means" of age verification and the "acceptable forms or methods of identification." § 13-63-102(4). The Division has published a Proposed Rule that would implement the Act's age-verification requirements. *See* Utah Social Media Regulation Act Rule, 20 Utah State Bulletin 15 (Oct. 15, 2023) (to be codified at Utah Admin. Code R152-63), https://perma.cc/FH7X-HCZC ("Proposed Rule"). The Proposed Rule makes those constitutional burdens worse, not better.

64. The Act's text does not mention identity verification. But to determine whether a specific person is the age he says he is, covered websites may also need to determine the identity of that individual. It may not be enough to simply verify the age of whatever person may be listed on a form of identification (if the person even has such a record) because that record may not
accurately reflect who the individual actually is. Thus, the Act may also require covered websites to verify at least some account holders' identities—including adults—as a precondition to those account holders' access to members' websites. And the Act's steep penalties for noncompliance may inspire covered websites to verify the identities of all account holders just to be safe. Likewise, parents cannot provide consent without identifying themselves and their children.

65. The Proposed Rule further suggests that the Act requires identity verification, as it requires covered websites to "proactively identify" all users. Proposed Rule at R152-63-4(2). Any steps that a covered website takes to "proactively identify" minors will necessarily lead that company to "proactively identify" adult users, too. Id. That is because "proactive[]" identification under the Rule involves account holders who claim to be adults.

66. Age verification requires people to provide identification or personal information to gain access to protected speech on covered websites. As a result, some will be deterred from using covered websites because they are unwilling or unable to provide that identification or personal information. Those who are not deterred must "forgo the anonymity otherwise available on the internet" as the state-imposed price of admission. Griffin, 2023 WL 5660155, at *17 (quoting Am. Booksellers Found. v. Dean, 342 F.3d 96, 99 (2d Cir. 2003)); see ACLU v. Mukasey, 534 F.3d 181, 197 (3d Cir. 2008) ("relinquish the anonymity to access protected speech").

67. Parental consent. Once a covered website verifies a new or existing account holder as a minor, the company must "confirm that a minor has [parental] consent" to hold an account. § 13-63-102(3)(a). If a company is unable to "confirm" that the minor has such consent, the company must "deny access to the account." § 13-63-102(3)(b); see § 13-63-102(1). "Minors" are all users younger than 18, except for those who are "emancipated [or] . . . married." § 13-63-101(7).

68. The Act also directs the Division "to establish processes or means to confirm that a parent or guardian has provided consent for the minor to open or use an account." § 13-63-102(3)(d). The Division has described such a process in the Proposed Rule: "(a) using a method that complies with 16 CFR 312.5(b)(2) or (3), or has been approved by the Federal Trade Commission . . . ; and (b) obtaining a written attestation from the parent or guardian that they are the minor's legal guardian." See Proposed Rule at R152-63-6. The Federal Trade Commission has provided that websites can secure parental consent in a number of ways, including (1) signing a consent form; (2) using a credit card or debit card; (3) having a parent call a number "staffed by trained personnel"; (4) having a parent "connect to trained personnel via video-conference"; and (5) checking a parent's government identification "against databases of such information" (where the website must delete the identification afterward). 16 C.F.R. § 312.5(b)(2)-(3).

69. The Act does not account for the difficulty in verifying a parent-child relationship, which entails verifying the identities of the minor and parent—*and* the relationship between them. In enjoining a similar requirement, the Western District of Arkansas credited the *State's* expert testimony that "the biggest challenge you have with parental consent is actually establishing . . .the parental relationship." *Griffin*, 2023 WL 5660155, at *4. These difficulties are compounded when families have differences in name or address, or where parents disagree about consent.

…

121. Plaintiff incorporates all prior paragraphs as though fully set forth herein.

122. The Act's requirements for age verification and parental consent (§ 13-63-102) are unconstitutional and cannot satisfy any form of First Amendment scrutiny. 123. Under the First Amendment, Defendants have the burden to "specifically identify"
how the Act addresses "an actual problem in need of solving. " Brown, 564 U.S. at 799. Strict scrutiny demands that "the curtailment of free speech must be actually necessary to the solution." Id. (citation omitted). Here, Defendants must demonstrate that there is a problem in need of governmental solution, as compared to private, family solutions. Parents have a wealth of choices to help oversee their minor children online, and those choices provide families more flexibility than
the State's one-size-fits-all mandate. Defendants cannot demonstrate why the Legislature ignored those viable alternatives. There are no legislative findings sufficient to justify the law's infringement on First Amendment rights. Edenfield v. Fane, 507 U.S. 761, 770 (1993).

124. **Parental-consent requirement.** The Act's parental-consent requirement is unconstitutional.

125. The Supreme Court has rejected the idea "that the state has the power to prevent children from hearing or saying anything without their parents' prior consent," because "[s]uch laws do not enforce parental authority over children's speech and religion; they impose governmental

B. To provide express consent pursuant to subsection a. of this section, the parent or guardian of a minor shall provide the parent or guardian's government-issued identification and credit card information to the social media company and consent to a fee of not more than 35 cents to be charged to the credit card provided.[3]

3. A. A social media company shall verify the age of an existing or new New Jersey account holder and, if the existing or new account holder is a minor, confirm that a minor has obtained expressed consent from the parent or guardian of the minor pursuant to subsection a. of section 2.[4]

4. For a social media platform account held by a New Jersey minor account holder, a social media company: …

b. shall not collect or use any personal information from the posts, content, messages, text, or usage activities of the account other than information that is necessary to comply with, and to verify compliance with, State or federal law, which information includes a parent or guardian's name, a birth date, and any other information required to be submitted pursuant to subsection b. of section 2.[5]

---

authority, subject only to a parental veto." *Brown*, 564 U.S. at 795 & n.3. That was true even in *Brown*, where California attempted to prohibit minors from purchasing violent video games. *See id.* at 818 (Alito, J., concurring in the judgment) ("the violence is astounding").

126. Minors' protections should therefore apply with special force to the covered websites here, which disseminate and facilitate a broad range of protected speech. That is, in part, why courts have held that parental-consent requirements for minors to use "social media" websites violate the First Amendment. *Griffin*, 2023 WL 5660155, at *18.

127. Moreover, the Act's one-size-fits-all approach requiring all minors at every development stage—from websites' youngest users to seventeen-year-olds—to secure parental consent is vastly overbroad. Even in the context of unprotected obscenity for minors, the Supreme Court has recognized that state laws that extend age-verification and parental-consent requirements to older minors raise even greater concerns. *Reno*, 521 U.S. at 866. The Act's exemption for married minors cannot further any state interest in the protection of minors. § 13-63-101(7)(b).

128. **Age-verification requirement.** The Act's age-verification requirement is also unconstitutional.

129. The Supreme Court has long held that a State cannot require individuals to provide personal information to access protected speech. *See, e.g.*, *Ashcroft*, 542 U.S. at 667 ("[A]dults without children may gain access to speech they have a right to see without having to identify themselves or provide their credit card information"); *Reno*, 521 U.S. at 874 (similar). Lower courts, too, have consistently rejected age-verification requirements. *See, e.g.*, *Mukasey*, 534 F.3d at 196-97; *PSINet, Inc. v. Chapman*, 362 F.3d 227, 236-37 (4th Cir. 2004).

130. Even if focusing only on the Act's impact on minors, the Act is unlawful. Age-verification requirements imposed on "social media" websites "obviously burden[] minors' First Amendment Rights." *Griffin*, 2023 WL 5660155, at *17. If the government cannot impose age-verification requirements to prevent minors from accessing unprotected speech (like obscenity for minors), the government certainly cannot require age-verification requirements that would impede minors' and adults' abilities to access a vast range of unquestionably protected speech.

[3] *Id.*

[4] *Id.*

[5] 13. *Fourth*, the Act's ban on "collect[ing] or us[ing] any personal information" from minors, § 13-63-103(4), violates the First Amendment because its purpose and effect is to restrict speech. Governmental restrictions of the "availability and use" of information raise grave First Amendment concerns. *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570-71 (2011). That is especially true here, where covered websites use the information they collect to make their expressive services functional and secure—and to display expressive content to users. The Act's failure to define what "personal information" the ban regulates also renders this provision unconstitutionally vague.

…

49. **Covered websites' collection and use of data.** The websites that NetChoice's members operate would be unusable if they could not collect, store, and use information and data that users provide. At the outset, covered websites collect certain demographic data to ensure that users are presented with age-appropriate content. Similarly, websites collect information about IP address, device type, operating system, screen resolution, browser type, language preferences, and time zone to determine how to present content (like choosing the correct format of a video

based on device type and screen resolution). User data is also necessary for deterring and detecting malicious actors, protecting users from would-be identity thieves, and maintaining overall security. Many websites also log activity and changes on an account. These logs help websites detect behavior that could signal a compromised account, and they can also help users restore accounts. Logs are also a crucial tool for law enforcement in many contexts. For instance, activity logs can help determine a missing person's last known location, interactions, or travel plans. Beyond these baseline functions, websites collect and use information about a person's usage to help personalize experiences on the websites. This aims to ensure that people see the content they want to see while avoiding content they do not want to see.

50. **Covered websites' dedication to beneficial user experiences and user security.** Safety and security are a paramount concern for NetChoice's members. They expend vast resources—time, money, and human resources—into improving their services and curating the content on their services to best ensure that it is appropriate for adults and minors alike. Members restrict the publication of content they consider harmful, like violent and sexual content, bullying, harassment, and content that encourages body shaming or eating disorders. Conversely, many covered websites promote age-appropriate content and positive content. For example, many promote content that encourages a positive self-image or that encourages being a good person through modeling respect or healthy habits. Covered websites implement these policies using a mix of human review, human-programmed computer algorithms, and automated editing tools.

51. Many NetChoice members also allow users to further curate the content they see. For instance, users can choose who they follow, block people, and control who sees and interacts with their content. Additionally, some members allow users to block categories of content. TikTok users, for example, can opt into "restricted mode," which automatically filters certain content and permits users to tailor the content they see with keyword filters (*e.g.*, not showing content featuring terms like "diet"). Facebook users can alter the content that Facebook recommends by hiding certain types of content or opting to see fewer posts from a specific person or group. Instagram users can select a "not interested" button to filter out content they do not wish to see. YouTube allows users to "dislike" content and to inform the service not to recommend certain content.

52. Many covered websites also restrict messaging between minors and adults. TikTok bans users under age 16 from sending or receiving direct messages, and it allows parents and guardians of 16- to 18-year-old users to restrict who can send messages to their teen, or to turn off direct messaging completely through its family pairing feature. For 16- and 17-year-olds, TikTok also turns off direct messaging by default. Facebook, Instagram, Snapchat, and Pinterest take other steps to restrict messaging between unconnected adults and teens. By default, Snapchat allows messages only between friends. And Snapchat does not recommend minors as suggested friends unless the person is already in their phone contacts or shares mutual friends. Instagram encourages teens via prompts and safety notices to be cautious in conversations with adults, even those to whom they are connected. And YouTube does not offer private messaging between users at all.

53. As explained above, these tools and others rely on user data.

…

72. *Ban on collection and use of personal information.* A covered website "shall not collect or use any personal information from the posts, content, messages, text, or usage activities of [a minor's] account other than information that is necessary to comply with, and to verify compliance with, state or federal law." § 13-63-103(4). Yet all Internet websites must collect *some* information to make services functional, secure, and social, and to provide age-appropriate experiences. Worse—and as with many other key terms—the Act does not define "personal information," "content," "usage activities," or any of the other operative terms in § 13-63-103(4).

…

171. Plaintiff incorporates all prior paragraphs as though fully set forth herein.

172. The Act's ban on collecting and using information from minors' accounts (§ 13-63-103(4)) is unconstitutional and cannot survive any form of First Amendment scrutiny.

173. The ban forbids a large range of activity that websites commonly engage in to facilitate their dissemination of speech and the facilitation of user expression. *See, e.g.*, *Bonta*, 2023 WL 6135551, at *16. At the outset, websites must collect information about users' ages to provide age-appropriate experiences for those users. Furthermore, many websites engage with users to learn about their preferences, use collected information to support personalized advertising, and recommend relevant user-generated content including music, film, educational content, and articles, among others. The First Amendment protects all of that. *See, e.g.*, *Sorrell*, 564 U.S. at 558.

174. By limiting the information that websites can collect, the ban also limits websites' ability to exercise meaningful editorial discretion by disseminating content that users find most relevant and prevents users from receiving this curated content. *See Tornillo*, 418 U.S. at 258.

175. The ban also triggers strict scrutiny because it would require covered websites to make their services functionally inaccessible to minors. *See Brown*, 564 U.S. at 799.

176. Utah does not have any sufficient governmental interest in preventing websites from collecting and using information necessary to improve websites' functionality, reliability, safety features, and overall usefulness for users.

177. The State cannot demonstrate what purported problem this ban responds to, how the ban is necessary to solve the purported problem, or why the existing and plentiful choices of private tools available to parents are insufficient to address any purported problem.

178. This ban is also not properly tailored.

179. The ban is overinclusive by covering the very information that makes websites useful, accessible, and secure. Prohibiting using "personal information" (which the Act does not define) could include information necessary to make the websites *functional* (like device type) and information that makes the websites *useful*.

180. Additionally, the ban is overinclusive because it fails to account for the differences among minors of different ages.

5. A. The division shall receive consumer complaints alleging a violation of, investigate alleged violations of, and enforce P.L. , c. (C.) (pending before the Legislature as this bill) as outlined in this section. All civil penalties in this section shall be collected by the director in a summary proceeding before a court of competent jurisdiction pursuant to the provisions of the "Penalty Enforcement Law of 1999," P.L.1999, c.274 (C.2A:58-10 et seq.). b. Subject to the conditions of subsection d. of this section, the director may impose a civil penalty in an amount not to exceed $2,500 for each violation of P.L. , c. (C.) (pending before the Legislature as this bill). c. Subject to the conditions of subsection d. of this section, the director may initiate a civil action to enforce P.L. , c. (C.) (pending before the Legislature as this bill) in the Superior Court. (1) A court presiding in an action initiated pursuant to this subsection may: 26 (a) declare that an act or practice constitutes a violation of P.L …

   Notwithstanding any provision of this section to the contrary, the division may initiate a civil action pursuant to subsection c. of this section against a person that: (a) fails to cure a violation after receiving notice pursuant to paragraph (1) of this subsection; or (b) commits another violation of the same provision of P.L. , c. (C.) (pending before the Legislature as this bill) after meeting the conditions of paragraph (2) of this subsection for a prior noticed violation.[6]

---

181. The ban is also underinclusive because many websites not covered by the Act that contain similar—if not the same—content will be able to collect and use this same information.

182. Even "the compelling and laudable goal of protecting children does not permit the government to shield children from harmful content by enacting greatly overinclusive or underinclusive legislation" that prohibits websites from collecting "personal information" from a "child." *Bonta*, 2023 WL 6135551, at *16 (granting preliminary injunction against state law that prohibited websites from collecting data from minors).

183. Unless declared invalid and enjoined, Utah Code § 13-63-103(4) will unlawfully deprive Plaintiff's affected members and Internet users of their First Amendment rights and will irreparably harm Plaintiff, its members, and Internet users.

[6] 75. Although the Act allows websites to "cure[]" first-time violations of a particular provision, that is of limited utility because it can be construed as essentially a single-use defense. No such defense potentially exists if the website again "commits another violation of the same provision"—even if the later violation is different in kind. § 13-63-202(4)(c)(ii). Thus, for example, a website's first-time failure to verify a minor's age would not create liability, but any subsequent failures to verify *any* minor's age could create liability, even if it had an entirely different cause. That is because a single statutory "provision" requires websites to verify age. *See* § 13-63-102(3)(a). Thus, depending on how it is construed, this ability to "cure" may provide covered websites with little protection from liability.

76. Covered websites also face private liability. The Act also grants a private right of action that allows individuals to enforce the Act's general requirements. § 13-63-301.

…

80. The Act provides a series of potentially illusory defenses to these broad and vague prohibitions. First, the Act's design requirements purportedly do not "impose liability" for: (1) "content that is generated by an account holder"; (2) content that is "created entirely by a third party" and which a company "passively display[s]"; (3) "information or content for which the social media company was not, in whole or in part, responsible for creating or developing"; or (4) "any conduct by a social media company involving a Utah minor account holder who would otherwise be protected by federal or Utah law." § 13-63-401(4). These purported defenses offer little certainty, given that "passively display[]" and other key terms are undefined. In any event, the purported distinction between "design" and "content" is also exceedingly difficult to apply. *Id.*

81. Second, to avoid potentially ruinous penalties for violating the Act, a covered website must (1) conduct "at least quarterly audits" to "detect practices, designs, or features that have the *potential* to cause or *contribute* to the addiction of a minor user"; and (2) "correct . . . any practice, design, or feature discovered by the audit to present more than a *de minimus* risk of violating" the design requirements. § 13-63-401(3)(b) (emphases added).

82. A company violates the Act if it fails to correctly predict and address any "practice, design, or feature" that has more than a "*de minimus*" risk of having the potential to cause or contribute to "addiction" for even a single minor. Violations trigger potential liability of: "(i) a civil penalty of $250,000 for each practice, design, or feature shown to have [violated the Act's design requirements]; and (ii) a civil penalty of up to $2,500 for each Utah minor account holder who is shown to have been exposed to [any such] practice, design, or feature[.]" § 13-63-401(3). The Division has authority to "administer and enforce" these requirements. § 13-63-401(1).

83. Thus, if a website violates the Act's design requirements for even *one* minor, then the website, conceivably, can be construed as liable for *every* minor who was exposed to the practice, design, or feature—regardless of a minor's age, parental consent, or individual circumstances.