Carl Szabo
Vice President & General Counsel, NetChoice
1401 K Street NW, Ste 502
Washington, DC 20005

NetChoice
Defending Free Speech and Free Enterprise Online

Comments on Department of Legal Affairs' Notice of Proposed Rule on the Florida Digital Bill of Rights

COMMENT

May 2, 2024

Department of Legal Affairs
Comment of NetChoice

Comments of NetChoice on Department of Legal Affairs' Notice of Proposed Rule on the Florida Digital Bill of Rights

Introduction

NetChoice submits these comments in response to the Department of Legal Affairs' Notice of Proposed Rule on the Florida Digital Bill of Rights ("Proposed Rule"). As a leading advocate for free speech and free enterprise online, NetChoice has serious concerns about several provisions in the Proposed Rule that raise significant First Amendment issues and conflict with existing federal law.

The Definition of "Willful Disregard" Raises First Amendment Concerns

The Proposed Rule's definition of "willful disregard" is deeply problematic from a constitutional perspective. By tying the concept of willful disregard to a failure to perform "reasonable age verification," the rule effectively mandates age verification as a precondition for online speech. This raises serious First Amendment concerns.

The Supreme Court has repeatedly held that content-based restrictions on speech are presumptively unconstitutional.[1] Requiring age verification for online services would likely be seen as an impermissible content-based restriction, as it would restrict access to lawful speech based on the age of the recipient.[2] The Proposed Rule's age verification mandate is not narrowly tailored to advance a compelling government interest, as required under strict scrutiny.[3]

[1] *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015).
[2] *See ACLU v. Gonzales*, 478 F. Supp. 2d 775 (E.D. Pa. 2007), *aff'd sub nom. ACLU v. Mukasey*, 534 F.3d 181 (3d Cir. 2008).
[3] *See FEC v. Wis. Right to Life, Inc.*, 551 U.S. 449, 464 (2007).

Moreover, the definition of "reasonable age verification" is itself troubling, as it incorrectly assumes that the government and businesses regularly engage in age and identity verification online. This is simply not the case. While age verification may be common in face-to-face interactions, such as purchasing alcohol or entering a bar, it is far from standard practice in the online context.[4] Imposing such a requirement on digital services would be unduly burdensome and potentially unconstitutional.[5]

The Proposed Rule's age verification requirement is also underinclusive, further undermining any claim that it is narrowly tailored. The rule appears to apply only to businesses that collect personal information online, leaving offline data collection practices unregulated. This arbitrary distinction further shows that the age verification mandate is not a properly tailored solution to protecting children online.[6]

In addition to the tailoring problems, the age verification requirement likely violates the First Amendment by functioning as an unconstitutional condition on speech. The government may not require individuals to relinquish their free speech rights as a condition of receiving a governmental benefit, such as the ability to operate a website.[7] By conditioning an online service's ability to engage in lawful speech on the implementation of an age verification system, the Proposed Rule runs afoul of this doctrine.[8]

The onerous age verification requirement, combined with the rule's vague and expansive definition of "willful disregard," will significantly chill the free speech of Floridians. The fear of liability based on an unintentional failure to accurately estimate a user's age will lead online services to engage in cautious self-censorship and over-restrict access to lawful content.[9] This sweeping regulatory burden on digital speech cannot be squared with basic First Amendment protections.

The "Reasonable Parental Verification" Requirement Conflicts with COPPA

The Proposed Rule's "reasonable parental verification" requirement also raises significant legal concerns, as it goes far beyond what is required under the federal Children's Online Privacy Protection Act (COPPA) and is likely preempted. COPPA's parental consent requirements are carefully tailored and do not mandate the kind of extensive documentation contemplated by the Proposed Rule.[10]

---

[4] *See Backpage.com, LLC v. McKenna*, 881 F. Supp. 2d 1262, 1279 (W.D. Wash. 2012).
[5] *See id.* at 1278-79.
[6] *See ACLU v. Reno*, 31 F. Supp. 2d 473, 497 (E.D. Pa. 1999), aff'd, 217 F.3d 162 (3d Cir. 2000), vacated sub nom. *Ashcroft v. ACLU*, 535 U.S. 564 (2002).
[7] *See Agency for Int'l Dev. v. Open Soc'y Int'l, Inc.*, 570 U.S. 205, 214 (2013).
[8] *E.g., NetChoice v. Griffin*, 2023 WL 5660155 (W.D. Ark.) (Aug. 31, 2023) (enjoining age-verification requirements for social media websites under the First Amendment); *NetChoice v. Bonta*, 2023 WL 6135551 (N.D. Cal.) (Sep. 18, 2023) (enjoining age estimation requirements for websites under the First Amendment); *NetChoice v. Yost*, 2024 WL 555904 (S.D. Ohio) (Feb. 12, 2024) (enjoining parental consent requirements to access websites under the First Amendment).
[9] *See Reno v. ACLU*, 521 U.S. 844, 871-72 (1997).
[10] 15 U.S.C. § 6501(9); 16 C.F.R. § 312.5.

Under the Proposed Rule, businesses must obtain "documents or information sufficient to evidence [the parental] relationship" before allowing children to exercise their privacy rights.[11] This could require demanding items such as birth certificates, court orders, or even DNA tests to confirm a parental relationship. Such a requirement is not only impractical but also inconsistent with COPPA's more flexible approach to parental consent.

COPPA allows operators to obtain parental consent through a variety of methods, including having the parent reply by email, participate in a telephone call, or use a credit card in connection with the transaction.[12] Importantly, COPPA does not require operators to collect additional documentary evidence of the parental relationship. The FTC has specifically rejected calls to limit the acceptable consent methods to those that require additional offline contact or verification, noting the importance of maintaining flexibility and supporting innovation in parental consent technologies.[13]

The Proposed Rule collides with federal COPPA law.

The conflict between the Proposed Rule's rigid parental verification requirement and COPPA's more adaptable approach creates a serious preemption problem. Under the Supremacy Clause of the U.S. Constitution, state laws that interfere with or are contrary to federal law are invalid.[14] COPPA expressly preempts inconsistent state laws regarding the online collection of personal information from children. By imposing more stringent and burdensome parental verification requirements than those in COPPA, the Proposed Rule likely crosses the line into preempted territory.

Even if the Proposed Rule's parental verification requirement is not facially preempted, it would still be invalid as applied under the doctrine of obstacle preemption. Obstacle preemption occurs when a state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."[15] Here, the Proposed Rule's onerous parental verification requirement would undermine COPPA's goal of providing operators with flexibility in obtaining parental consent and supporting innovative consent methods. By effectively banning commonly used consent methods, such as email, and requiring extensive additional documentation, the Proposed Rule erects an impermissible obstacle to the achievement of COPPA's purposes.

To the extent that the Proposed Rule contemplates imposing parental consent requirements on teens, the Proposed Rule faces additional COPPA preemption problems. COPPA's parental consent requirements only apply to minors twelve and under. If, under the Proposed Rule, parental consent requirements are imposed on teens, the Rule will conflict with and frustrate COPPA's purpose.

[11] Rule 2-3.003(1)(d) & (5).
[12] 16 C.F.R. § 312.5(b).
[13] Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972, 3991 (Jan. 17, 2013).
[14] *See* Preemption; constitutional clauses. Article VI, Paragraph 2 of the U.S. Constitution.
[15] *Freightliner Corp. Myrick*, 514 U.S. 280, 287 (1995).

COPPA already provides strong protections for children's online privacy. Under COPPA, operators must notify parents and obtain verifiable parental consent before collecting children's personal information.[16] COPPA also gives parents the right to review and delete their children's information, and to withdraw their consent at any time.[17] These protections are further enforced through the FTC's COPPA Rule and the agency's active enforcement efforts. Given this comprehensive federal framework, there is no need for Florida to impose additional, conflicting requirements on the collection of children's data.

Data Security Requirements Raise Additional First Amendment Concerns

Any data security scheme should be neutral or agnostic toward the framework businesses employ to implement the scheme's objectives. Framework agnosticism helps ensure that smaller businesses aren't burdened by requirements only achievable by larger players and leaves room for innovation and the adoption of better systems over time. Florida can build in this sort of framework agnosticism by requiring that data security practices "reasonably conform" with the standards set by NIST. Indeed, Tennessee adopted a similar approach in its data privacy law. To further alleviate concerns, the Proposed Rule could also:

- Clarify that Section 2-3.002(2)(d) applies only to *personal* data as opposed to *all* data;
- Section (3)(c) collides with 3(d) and should be removed;
- Clarify precisely what "duties" Section 2-3.002(3)(e) refers to.

As it stands, the Proposed Rule's data security provisions raise broader First Amendment concerns. In particular, the requirement that controllers implement "procedural safeguards" and provide staff training on deidentification raises concerns about compelled speech and burdens on protected expression.

Under the Proposed Rule, businesses would have to create specific types of employee training materials in order to share deidentified information. Creating and disseminating such training materials would undoubtedly involve expressive editorial choices that are protected by the First Amendment. The Supreme Court has long recognized that the First Amendment protects not only the right to speak, but also the right to decide "what not to say."[18] Government mandates that compel organizations to express specific messages or viewpoints violate this core First Amendment principle.[19]

The Proposed Rule's compelled training requirement is similar to other "disclosure" mandates that courts have struck down on First Amendment grounds. For instance, in *National Institute of Family & Life Advocates v. Becerr*a, the Supreme Court invalidated a California law requiring crisis pregnancy centers to post notices about the availability of state-funded abortions.[20]

---

[16] *See* 15 U.S.C. § 6501(9); 16 C.F.R. § 312.5.
[17] *Id.*
[18] Harvard Law. Rev. *Two Models of the Right to Not Speak*, 133 Harv. L. Rev. 2359 (May 2020).
[19] *Id.*
[20] *National Institute of Family & Life Advocates v. Becerra*, 585 US _ (2018).

The Court held that the law unconstitutionally compelled the centers to speak a message contrary to their viewpoint. Similarly, in *Washington Post v. McManus*, the Fourth Circuit struck down a Maryland law requiring newspapers and other online platforms to post information about the political ads they run.[21] The court found that the law compelled political speech and forced publishers to make editorial judgments about which content required the disclaimer.

The Proposed Rule's viewpoint-based regulation of private entities' speech cannot survive First Amendment scrutiny.

Like the laws at issue in *NIFLA* and *McManus*, the Proposed Rule's training mandate compels organizations to draft and present content expressing a specific viewpoint about data privacy and security. Organizations that disagree with the rule's particular approach to data deidentification would nevertheless have to endorse those views in compulsory employee trainings or face liability. Such viewpoint-based regulation of private entities' speech cannot survive First Amendment scrutiny.

The Proposed Rule's training requirement also interferes with protected editorial discretion about how best to secure user data. As the Supreme Court has recognized, choices about content are entitled to the same First Amendment protections as the publishing decisions of newspapers and broadcasters.[22] Editorial decisions about data security measures are no exception.

Just as the First Amendment protects a newspaper's choices about which kind of lock to place on its office doors, it protects an online service's decisions about how to protect user information. By rigidly mandating specific training on the Rule's debatable interpretation of deidentification, the Rule infringes on this protected editorial discretion over security procedures.

Enforcement Procedures Must Incorporate First Amendment Safeguards

Beyond its substantive flaws, the Proposed Rule also lacks critical procedural safeguards needed to ensure enforcement actions comport with due process and the First Amendment. Most glaringly, the Rule fails to provide a clear and prompt avenue for judicial review of cease-and-desist orders and other administrative sanctions.

It is black-letter First Amendment law that speech licensing schemes must ensure prompt judicial review of administrative decisions denying the right to speak.[23] Without such safeguards, the mere threat of prolonged or costly enforcement proceedings can impermissibly chill protected expression. Yet the Proposed Rule imposes no deadline on the Department's investigations and allows sanctions to take

[21] *The Washington Post v. McManus*, No. 19-1132 (4th Cir. 2019).
[22] *Brown v. Entertainment Merchants Association*, 564 US _ (2011).
[23] *See,* Carl Brody, *Prompt Judicial Review Of Administrative Decisions: Providing Due Process In Unsure Waters*, FL Bar Journal Vol. 87 No. 4 (2013).

effect before judicial review. This regime of open-ended administrative discretion plainly violates the First Amendment's command that any restraint in advance of a final judicial determination on the merits must be limited to preservation of the status quo for the shortest period compatible with sound judicial resolution.[24]

The Rule's deficient judicial review procedures cannot be justified based on judicial economy, administrative convenience, or the state's interest in protecting children. As the Supreme Court explained in *Freedman v. Maryland*, a censorship system creates special dangers and requires rigorous procedural safeguards, even if enacted in the name of protecting minors.[25] The Court further emphasized that only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression.[26] The Proposed Rule plainly fails this standard by allowing administrative orders restricting speech without prompt and definite access to judicial oversight.

The Rule's lack of meaningful judicial review is exacerbated by the vagueness of key provisions, which provide the Department with virtually unchecked discretion to sanction disfavored speakers. For example, the Rule allows the Department to ban an operator based on a mere “likelihood” of undisclosed future violations — an amorphous and subjective standard that invites arbitrary enforcement.

The Proposed Rule hands over incredible control of individuals’ rights and freedoms to the government.

Similarly, the Rule empowers the Department to impose additional conditions on an operator's data privacy practices whenever the Department deems it "necessary," without further definition or constraint. Such open-ended grants of regulatory discretion do not provide the "narrow, objective, and definite standards" the First Amendment demands for speech licensing schemes.

The Proposed Rule also fails to include even rudimentary checks on administrative favoritism and retaliation. The Rule's procedures allow a single agency official to initiate investigations, adjudicate violations, impose sanctions, and even speak publicly about a case before the target has notice or opportunity to respond.

There are no restrictions on ex parte communications between agency staff and Department decision-makers, no mandatory recusal process for biased officials, and no formal rules of evidence or discovery. This absence of basic due process protections renders the Rule's enforcement procedures fundamentally incompatible with the First Amendment's promise of freedom from censorship and the right to disseminate speech.

---

[24] *Freedman v. Maryland*, 380 U.S. 51, 58 (1965).
[25] *Id.*
[26] *Id.*

Accordingly, the enforcement procedures in the Proposed Rule must be substantially revised to incorporate essential First Amendment safeguards. At minimum, the Rule should be amended to:

1. impose hard deadlines on Department investigations;
2. require prompt notice and opportunity to respond for enforcement targets;
3. provide a clear avenue for pre-enforcement judicial review;
4. adopt narrow and objective standards constraining the Department's discretion; and
5. ban biased and retaliatory exercises of Department authority.

Absent these critical revisions, the Rule's enforcement regime cannot be reconciled with basic constitutional protections for free speech and due process.

Conclusion

While we appreciate the Department's efforts to protect Floridians' privacy rights, the Proposed Rule is plagued by serious constitutional defects that cannot be ignored. The Rule's sweeping age verification mandate and rigid parental consent requirement plainly violate the First Amendment and conflict with governing federal law. At the same time, the Rule's flawed data security provisions impermissibly burden editorial discretion and compel speech in service of outmoded regulatory standards. And the Rule's enforcement procedures fail to include basic safeguards against censorship and administrative abuses.

Given these fatal flaws, the only reasonable course is to substantially revise the Proposed Rule to cure its constitutional defects and tailor its requirements to accord with the First Amendment and federal law. We urge the Department to undertake this essential process of revision and to meaningfully engage with stakeholders in crafting a more legally sustainable approach to protecting privacy.

By promoting an innovation-friendly, enforcement-centric approach grounded in existing legal frameworks, the Department can position Florida for success in the algorithmic age while safeguarding consumer welfare. We look forward to continued engagement with the Department and other stakeholders in pursuit of these vital objectives.

Respectfully submitted,

Carl Szabo
Vice President & General Counsel
NetChoice

NetChoice is a trade association that works to make the internet safe for free enterprise and free expression.[27]

[27] *The views of NetChoice do not necessarily represent the views of its members.*