March 8, 2024

The Honorable Ron DeSantis, Governor of Florida
Florida State Capitol
400 South Monroe Street
Tallahassee, FL 32399-0001

Re: HB 3 - "Online Access to Materials Harmful to Minors" (Veto Request)

Dear Governor DeSantis:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully request a veto on HB 3.

CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] CCIA holds a firm conviction that children are entitled to a higher level of security and privacy in their online experiences. Presently, our members are actively engaged in various initiatives to integrate robust protective design features into their websites and platforms.[2] CCIA's members have been leading the effort to implement settings and parental tools to individually tailor younger users' online use to the content and services that are suited to their unique lived experience and developmental needs. For example, various services allow parents to set time limits, provide enhanced privacy protections by default for known child users, and other tools to allow parents to block specific sites entirely.[3]

This is also why CCIA supports the implementation of digital citizenship curriculum in schools, to not only educate children on proper social media use but also help educate parents on what mechanisms presently exist that they can use now to protect their children the way they see fit and based on their family's lived experiences.[4] Florida has already taken important steps to adopt such an approach – just last year, the legislature passed HB 379, which requires training for online safety and social media. CCIA recommends allowing this law to have an opportunity to work by training students, parents, and teachers on online safety across the state.

It should also be recognized that protecting children from harm online does not include a generalized power to restrict ideas to which one may be exposed. Speech that is neither obscene to young people nor expressly illegal cannot be suppressed solely to prevent young online users from accessing ideas or images that a legislative body disfavors. Proposals to keep children safe online should be established through a risk-based approach to developing protections for different ages of users and by focusing on tangible harm.

---

[1] For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.
[2] Jordan Rodell, *Why Implementing Education is a Logical Starting Point for Children's Safety Online*, Disruptive Competition Project (Feb. 7, 2023), https://www.project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/.
[3] Competitive Enterprise Institute, *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/.
[4] *See supra* note 2.

CCIA understands that you have been working closely with lawmakers to address concerns originally included under HB 1. Unfortunately, CCIA remains opposed to the amended provisions now proposed under HB 3 regarding social media platforms. We encourage you to veto HB 3 as the following issues still remain.

HB 3 is likely to create unintended consequences that affect a wide range of services and features offered to consumers.

While HB 3 is framed as a measure to address online protections for younger users on social media platforms, the definition of "social media platform" is incredibly broad and likely to impact many online services that are not typically considered social media. This is further compounded by including the use of "push notifications or alerts sent by the online forum, website, or application to inform a user about specific activities or events related to the user's account" as an "addictive feature". It is unclear whether these notifications would include items such as notifications to consumers about when payments are due, whether a consumer wants to opt-in to certain services or features, or notifying a consumer that an application or security update is available.

HB 3's provisions regarding liability for age-specific requirements present concerns regarding privacy and feasibility.

While Section 501.1736, unlike the provisions most recently considered under HB 1, no longer expressly requires covered social media platforms to employ age verification tools for users, the age-specific requirements would still force companies to verify the age of users at the risk of otherwise facing liability for age-specific requirements.

Any commercially available age verification method that may be used by a covered platform carries serious privacy and security concerns for users. Notably, the Commission Nationale de l'Informatique et des Libertés (CNIL) analyzed several existing online age verification technologies but found that none of these options could satisfactorily meet three key standards: 1) providing sufficiently reliable verification; 2) allowing for complete coverage of the population; and 3) respecting the protection of individuals' data, privacy, and security.[5] The availability of a functional "anonymous age verification method" remains uncertain. Though the intention to keep kids safe online is commendable, this bill is counterproductive to that initiative by requiring more data collection about young people.

When businesses are required to verify a user's age, they are required to collect additional information. This is itself likely to conflict with data minimization principles inherent in typical federal and international privacy and data protection compliance practices. A recent study from the Pew Research Center found that many Americans worry about children's online privacy but when asked about who is responsible for protecting children's online privacy, most (85%) say parents hold a great deal of responsibility for protecting kids' online privacy. 59% also say that tech companies bear the responsibility while 46% believe the government does. The study also highlights why it is important to consider the tradeoffs associated with age

[5] *Online age verification: balancing privacy and the protection of minors,* CNIL (Sept. 22, 2022), https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.

verification and consent proposals that would require the additional collection of data; around 89% of Americans are very or somewhat concerned about social media platforms knowing personal information about kids.[6]

It is also unclear how enforcement may apply in instances where a user decides to use deceptive verification information such as using an identification card that is not their own. Additionally, it is unclear what impact users' employment of virtual private networks (VPNs)[7] and other mechanisms to avoid location-specification age verification requirements could have on organizations' liability under this bill. It does not advance the bill's goal to place covered companies in a Catch-22 where they cannot be fully compliant without incurring new liability.

Restricting access to the internet for younger users curtails their First Amendment right to information, denying them entry to supportive online communities that might be unavailable in their local physical location.

The Children's Online Privacy Protection Act (COPPA) and associated rules at the federal level currently regulate how to address users under 13, a bright line that was a result of a lengthy negotiation process that accounted for the rights of all users, including children, while also considering the compliance burden on businesses. To avoid collecting data from users under 13, some businesses chose to shut down various services when COPPA went into effect due to regulatory complexity — it became easier to simply not serve this population. While the proposed amendment would now restrict access for users under 14, rather than under 16, this is still a departure from COPPA and continues to present First Amendment concerns. Further, while the proposed amendment allows a user to "dispute the termination" of their account, the language also specifies that an account must be terminated within 90 days "if the account holder fails to effectively dispute the termination." There is no explanation of what would qualify as an "effective dispute." It is therefore unclear what instances would allow a user to maintain their account versus when a user's account would still face termination.

When businesses are required to deny access to social networking sites or other online resources, this may also unintentionally restrict children's ability to access and connect with like-minded individuals and communities. For example, in instances where children may be in unsafe households, this could create an impediment for children seeking communities of support or resources to get help.

The proposed amendment for HB 3 would now prohibit 14- and 15-year old users from being account holders on covered social media platforms unless the user's parent or guardian has provided consent. Serious concerns arise when verifying whether a parent or guardian is in fact a minor's legal parent or guardian. Many parents and legal guardians do not share the same last name as their children due to remarriage, adoption, or other cultural or family-oriented decisions. If there is no authentication that a "parent or guardian" is actually a minor's legal parent or guardian, this may incentivize minors to ask other adults who are not their legal parent or guardian to verify their age on behalf of the minor to become an account holder. It is

[6] Colleen McClain, *How americans view data privacy*, Pew Research Center: Internet, Science & Tech (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.
[7] Cristiano Lima, *Utah's porn crackdown has a VPN problem*, The Washington Post (May 5, 2023), https://www.washingtonpost.com/politics/2023/05/05/utahs-porn-crackdown-has-vpn-problem/.

also unclear who would be able to give consent to a minor in foster care or other nuanced familial situations, creating significant equity concerns. Further, scenarios where a legal parent or guardian is not located in Florida or is not a resident of the state creates significant confusion for consumers and businesses.

Age verification and parental consent requirements for online businesses are currently being litigated in several jurisdictions.

When the federal Communications Decency Act was passed, there was an effort to sort the online population into children and adults for different regulatory treatment. That requirement was struck down by the U.S. Supreme Court as unconstitutional because of the infeasibility.[8] After 25 years, age authentication still remains a vexing technical and social challenge.[9] California, Arkansas, and Ohio recently enacted legislation that would implement age verification and estimation requirements — each law is currently facing a legal challenge due to constitutional concerns, and judges recently put both laws on hold until these challenges can be fully reviewed.[10] The fate of a similar law in Utah is also in jeopardy as it is also facing legal challenges.[11] CCIA recommends that lawmakers permit this issue to be more fully examined by the judiciary before burdening businesses with legislation that risks being invalidated and passing on expensive litigation costs to taxpayers. The Florida House of Representatives Staff analysis[12] acknowledges these legal challenges and the likely constitutional issues that this bill presents, including the First Amendment right to freedom of speech. ***While we understand that both you and the legislature have worked to implement amendments aimed at addressing these constitutional issues, CCIA believes that those modifications fall far short of adequately doing so.***

* * * * *

While we share the concerns regarding the safety of young people online, we encourage you to resist signing legislation that is not adequately tailored to this objective, and we respectfully request a veto of HB 3.

We appreciate your consideration of these comments and stand ready to provide additional information related to technology policy.

Sincerely,

Khara Boender
State Policy Director
Computer & Communications Industry Association

[8] *Reno v. ACLU*, 521 U.S. 844 (1997).
[9] Jackie Snow, *Why age verification is so difficult for websites*, The Wall Street Journal (Feb. 27, 2022), https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728.
[10] *NetChoice, LLC v. Bonta* (N.D. Cal. 5:22-cv-08861); *NetChoice, LLC v. Griffin* (W.D. Ark. 5:23-cv-05105; *NetChoice, LLC v. Yost* (S.D. Ohio 2:24-cv-00047)).
[11] *NetChoice, LLC v. Reyes* (D. Utah 2:23-cv-00911).
[12] Florida House of Representatives Staff Analysis of FL HB 3, https://flsenate.gov/Session/Bill/2024/1/Analyses/h0001.RRS.PDF (Jan. 9, 2024).