May 2, 2024

Department of Legal Affairs
Attn: Edward Tellechea, Chief Assistant Attorney General
PL-01 The Capitol
Tallahassee, Florida 32399

Re: Implementing Regulations for the Florida Digital Bill of Rights Act

On behalf of the Computer & Communications Industry Association (CCIA), I write to express several concerns about the proposed regulations to implement the Florida Digital Bill of Right Act (Act).

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. 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]

CCIA and its members commend the Department for its efforts to implement the requirements under the Florida Digital Bill of Rights swiftly and transparently. However, CCIA has serious concerns about the proposed requirements, especially given the constitutional and implementation challenges presented by overly broad age-verification requirements. As discussed below, CCIA recommends the Department revise the proposed regulations to avoid raising constitutional and compliance concerns.

1. Section 2-3.002 — "Data Security"

Data security remains a difficult challenge for businesses as the threat landscape is constantly evolving with new emerging threats and vulnerabilities. Thus, any legislative approach to data security must provide businesses with sufficient flexibility so they can tailor their efforts toward the security risks most relevant to them and their customers. However, subsection (2)(b) specifies that a controller's data security practice must fully comply with the framework and standards specified by the National Institute of Standards and Technology or Department of Commerce. Given the varying threats and challenges, data security requirements need to be

[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/.

risk-based and not tied to any specific framework to avoid restricting businesses' ability to respond to threats. CCIA suggests amending the proposed language to require data security practices that *reasonably conform* with the risk management framework and standards to avoid this risk.[4] Further, the Department should make clear that requirements in (2)(d) only apply to "personal data" and not all data as currently written.

The proposed administrative data security practices in subsection (3) could also be strengthened. As currently written, subsection (3)(c) specifies that a controller must document "any breach" and subsection 3(d) further requires a controller to regularly test and monitor compliance with data security practices including " to detect actual or attempted attacks on, or intrusions into systems that contain personal data". Overly prescriptive documentation requirements risk imposing heavy compliance costs on businesses with no material countervailing benefits to the data security of consumers. Moreover, businesses daily face dozens if not hundreds of potential security threats and attempted intrusions. Requiring them to document any such attempt, even if it was unsuccessful due to robust security measures or mitigation tactics, would unnecessarily burden businesses with a check-box compliance exercise. Further, subsection 3(e) also creates some confusion as it vaguely permits authorized users to access such secure systems to perform "duties". CCIA recommends that the Department eliminate the requirement in 3(c) and clarify the reference to "duties" in subsection 3(e).

2. Section 2-3.003 — "Enforcement"

The enforcement provision as currently written provides businesses with little to no guidance on how to comply with the proposed requirements. To avoid the risk of liability, especially considering the possibility of treble damages, businesses will have no alternative other than to verify the age of any user, raising significant First Amendment concerns.

Age Verification Considerations. Section 501.705 of the Act provides individuals with certain consumer rights regarding their personal information including access, correction, deletion, but also the ability to opt-out of the processing of their personal data for targeted advertising, sale, or profiling. Section 2-3003(5) of the proposed regulations further describes that a controller in determining "whether someone is a parent entitled to exercise rights under" the Act, or for a known child, "shall conduct reasonable parental verification before allowing the exercise of any right." CCIA has serious concerns about this approach.

First, the proposed regulations do not specify whether the consent needs to be obtained from a teen or their parents which creates conflicts with other aspects of the Act. For instance, Section 501.715(1) describes that a business is required to obtain "affirmative authorization" before processing sensitive data, including of a "known child who is between 13 and 18 years of age." Notably, the Act does not specify that the affirmative authorization must come from a parent. However, Section 2-3.0003 could have a broader application that would extend beyond the rights provided by the statute around the processing of sensitive data. As a result, companies may be required to obtain "affirmative authorization" from a 13-17 year-old user in certain circumstances and from their parent or guardian in others.

[4] *See,* Tennessee Information Protection Act, 47-18-3213 (" A controller or processor has an affirmative defense to a cause of action for a violation of this part if the controller or processor creates, maintains, and complies with a written privacy policy that: *Reasonably conforms* to the [NIST] privacy framework").

Second, serious concerns arise when mandating businesses to verify 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. It is also not clear who would be able to give consent to a teen in foster care or other nuanced familial situations such as if the parent is not located in or a resident of Florida—creating significant equity concerns. As a result, there is a serious risk that businesses will be required to deny young people access to important online services and sites that enable them to research sensitive health-related issues or find communities of support if they are in an unsafe household.

Conflict with Federal Law. The proposed regulations regarding minors under the age of 13 would directly conflict with requirements under the Children's Online Privacy Protection Act and are likely preempted as a result.

COPPA's twin aims are to protect the privacy of children and support the development of high-quality appropriate content. The Federal Trade Commission has previously stated that the "primary goal of COPPA is to place parents in control over what information is collected from their young children online." While operators are generally required to obtain verifiable parental consent before the collection of any information from a child under the age of 13, the Rule provides several exceptions to the parental consent requirement.[5] One of the exceptions permits operators to collect online contact information about parents including an email or another similar identifier that allows for the physical or online contact of a specific person but phone numbers are explicitly excluded.[6]

The proposed regulations would directly conflict with COPPA in a few ways.

First, compliance with the "reasonable parent verification" requires businesses to collect "from the child the parent's name, address, phone number, and email address[.]" A business must then verify "that the parent is the child's parent by obtaining documents or information sufficient to evidence that relationship." The proposed rules further specify that a business must use any commercially reasonable methods to verify the "parent's identity and age."

It is unclear how a business is able to comply with the proposed requirements without violating the obligations under the COPPA Rule. While Section 501.703(3) states that compliance with COPPA's parental consent requirements is considered to be sufficient under the Act, this is still insufficient. The proposed parental consent requirements go beyond the COPPA limits on the collection of information and raises the age-gate by applying it to adolescents and teens.

Second, COPPA provides that no state or local government "may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter that is inconsistent with the treatment of those activities or actions under this section."[7] The proposed verifiable parental consent

[5] 15 U.S.C. § 6502(b)(2).
[6] 15 U.S.C. § 6501(12).
[7] 15 U.S.C. § 6502(d).

requirements, especially regarding users over the age of 12, likely are inconsistent and in conflict with COPPA's overall framework.[8]

CCIA strongly urges the Department to address these concerns and offers a few suggestions. Subsections (1) and (5) need to be amended to ensure that businesses are not required to obtain parental consent for individuals over the age of 13, preserving teens' ability to access these services. The Department should also clarify and limit the scope of the parental consent requirement for users under 13 to avoid conflict with COPPA. Specifically, the Department should make clear that the "reasonable parental verification" requirement is limited to situations only where a parent is required to provide consent for a minor, and not for all customer rights granted under the Act.

Knowledge Standard. This proposed standard for "willful disregard" creates a few serious problems for businesses.

The Act describes the "known child" standard to include actual knowledge but also includes an undefined "willfully disregard." Under proposed regulations, this would mean a controller, "based on the facts or circumstances readily available to [them], should reasonably have been aroused to question whether a consumer was a child and thereafter failed to perform reasonable age verification." The proposed regulations also specify that the Department "will not find a controller willfully disregarded a consumer's age if that controller utilizes a reasonable age verification method with respect to all of its consumers."

The proposed standard for "willful disregard" creates serious problems for businesses. It provides no meaningful clarity as to what facts or circumstances would "arouse the question" that a consumer is a "known child." From smart speakers to automated sprinklers, users including families rely upon numerous smart devices and home products for a variety of purposes. Importantly, many of these services and products are often used by all family members—including children and teens. The proposed regulations fail to account for this important consideration.

The concerns about the vagueness of the "willful disregard" standard are further compounded by its inclusion in the enforcement section that allows for trebled damages. As a result, the "willful disregard" standard will force businesses to conduct age verification of all consumers. Such a broad age verification requirement is a clear violation of the First Amendment. Arkansas, California, and Ohio recently enacted legislation to implement age-verification and estimation requirements but each law is facing a legal challenge due to constitutional concerns.[9] Further, courts have found similar age verification frameworks to be unconstitutional restrictions on accessing speech. For example, the District Court for the Northern District of California, after reviewing ten provisions of the California Age-Appropriate Design Code Act provisions, held that all ten likely violated the First Amendment.[10]

[8] *See*, *Jones v. Google*, No. 21-16281, 56 F.4th 735 (9th Cir. Dec. 28, 2022) (holding that COPPA preempts state laws that are "inconsistent with the statute's treatment of regulated activities").
[9] *See, NetChoice, LLC v. Griffin*, No. 5:23-CV-05105, 2023 WL 5660155 at *21 (W.D. Ark. Aug. 31, 2023); *NetChoice, LLC v. Yost*, No. 2:24-CV-00047, 2024 WL 555904 (S.D. Ohio Feb. 12, 2024).
[10] Alvaro Marañon, *NetChoice v. Bonta: First Amendment Challenges to Age-Gating Mandates*, Disruptive Competition Project (Oct. 16, 2023), https://www.project-disco.org/privacy/netchoice-v-bonta-first-amendment-challenges-to-age-gating-mandates/

The Department needs to make clear that a business deciding to not verify the age of its customer does not constitute a willful disregard that some of its users may have been minors. CCIA recommends the Department amend Section 2-30003(4)(a) and strike the language after "where a consumer was a child." This amendment would help address the uncertainty created by the vague "willful disregard" knowledge, especially considering the risk of potential trebled damages to businesses.

* * * * *

While we share the concerns of the sponsor and the Committee regarding the safety of young people online, we strongly encourage the Department to amend the proposed regulations in light of the concerns raised through these comments. We appreciate the consideration of these comments and stand ready to provide additional information as well.

Sincerely,

Alvaro Marañon
Policy Counsel, Privacy & Security
Computer & Communications Industry Association