November 1, 2023

Utah Department of Commerce
Division of Consumer Protection
Attn: Daniel Larsen
160 E 300 S
Salt Lake City, UT 84111

Re: Public Hearing on Proposed Rules for Social Media Regulation Act

Division of Consumer Protection:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully raise some concerns with the proposed rules for the Social Media Regulation Act.

CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] Proposed regulations on the interstate provision of digital services therefore can have a significant impact on CCIA members. Recent sessions have seen an increasing volume of state legislation related to the regulation of digital services. While recognizing that policymakers are appropriately interested in the digital services that make a growing contribution to the U.S. economy, these legislative efforts warrant further study, as they may raise constitutional concerns, conflict with federal law, and risk impeding digital services companies in their efforts to restrict inappropriate or dangerous content on their platforms.[2]

CCIA strongly believes children deserve an enhanced level of security and privacy online. Currently, there are numerous efforts among our members to incorporate protective design features into their websites and platforms.[3] CCIA's members have been leading the effort to raise the standard for teen safety and privacy across our industry by creating new features, settings, parental tools, and protections that are age-appropriate and tailored to the differing developmental needs of young people. For example, various services allow parents to set time limits, provide enhanced privacy protections by default for known child users, and other tools

[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] Taylor Barkley, Aubrey Kirchhoff, and Will Rinehart, *5 things parents and lawmakers need to know about regulating and banning social media*, The CGO (Mar. 7, 2023), https://www.thecgo.org/benchmark/5-things-parents-and-lawmakers-need-to-know-about-regulating-and-banning-social-media.
[3] 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/.

to allow parents to block specific sites entirely.[4] While CCIA strongly supports the overall goal of keeping children safe online, especially regarding social media, there are several overarching concerns we would like to raise about the Act.

First, any age verification measure comes with costly trade-offs for businesses and users alike, even more so for users from vulnerable communities. Although the proposed rules identify several methods for conducting age verification, the methods still face technical challenges, undermine the safety and privacy of their users, and conflict with data minimization principles. Notably, the Commission Nationale de l'Informatique et des Libertés (CNIL) analyzed several existing online age verification solutions but found that none of these options could sufficiently 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]

Secondly, age verification requirements may put Utahns, especially children and teens, at greater risk of harm. Specifically, CCIA is concerned with the mandate for businesses to proactively scan and collect age verification data, which would paradoxically force companies to collect a higher volume of data on users.[6] Businesses may be forced to accumulate personal information they do not want to collect and consumers do not want to give, and that data collection creates extra privacy and security risks for all users. This mandated data collection would include collecting highly sensitive personal information about children, including collecting and storing their geolocation to ensure they do not reside outside of the state when confirming their age.

The difficulty of operationalizing this mandate is further compounded by the additional requirement to accurately verify whether a "parent or guardian" is that specific 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 that specific 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 register for an account with a "large social media platform." It is 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 Utah or is not a resident of the state create significant confusion for consumers and businesses.

---

[4] *See* CCIA, *What Tools are Available to Families and Young People Online*, https://ccianet.org/wp-content/uploads/2023/02/General-Child-Safety-Mechanisms_Fact-Sheet.pdf.
[5] CNIL, *Online age verification: balancing privacy and the protection of minors,* (Sept. 22, 2022), https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.
[6] Caitlin Dewey, *California's New Child Privacy Law Could Become National Standard*, The Pew Charitable Trusts (Nov. 7, 2022), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/11/07/californias-new-child-privacy-law-could-become-national-standard

Thirdly, the Act also imposes vague and sometimes even conflicting requirements for covered platforms without any flexibility. A covered platform would be held liable for failing to perform age verification but they are also required to dispose of any identifying information about the user after verifying their age. However, by requiring covered businesses to delete relevant information, the law would leave businesses without a means to document their compliance. This becomes especially problematic in instances where a user decides to use deceptive verification information such as using an identification card that is not their own. Compliance is further made difficult by the lack of any reasonable deletion exceptions such as if it concerns fraud.

Ultimately, this Act would restrict access to important parts of the internet for many users, likely infringing upon the First Amendment right to access information, including access to supportive communities that may not be accessible forums in their physical location. 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.[7] After 25 years, age authentication continues to be a complex technical and social challenge.[8] Federal district courts have already enjoined similar youth online safety legislation from going into effect.[9]

Though the intention to keep kids safe online is commendable, this Act is counterproductive to this goal as it conditions internet access upon the sharing of more data about young users. CCIA believes an alternative to solving these complex issues is for lawmakers to work with all stakeholders, including younger users, families, and private businesses to help promote a safe online environment for all. Companies continue to innovate and implement new safety mechanisms such as daily time limits or child-safe searching so that families can choose how they want their children to safely navigate social media. This is also why CCIA supports the implementation of a digital citizenship curriculum in schools,[10] which would both educate children on proper social media use and empower parents by informing them of what mechanisms are already out there that they can use now to protect their children the way they see fit and based on their family's lived experiences.

[7] *Reno v. ACLU*, 521 U.S. 844 (1997).
[8] 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.
[9] 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/
[10] Edward Longe, Will Flanders, *A better way to protect teenagers online*, Wisconsin State Journal (Aug. 25, 2023), https://madison.com/opinion/column/a-better-way-to-protect-teenagers-online----will-flanders-and-edward-longe/article_683a2b94-42f2-11ee-9a79-a32fcbd2fedb.html.

We appreciate your consideration of these comments during this public hearing and look forward to providing further input as the Agency considers amendments to the Act in the coming months.

Sincerely,

Alvaro Marañon
Privacy Policy Counsel
Computer & Communications Industry Association