**February 4, 2025**

House Judiciary Committee
Post Office Box 11867
Columbia, South Carolina 29211

## Re: HB 3405 - "App Store Accountability Act" (Oppose)

Dear Chair Newton and Members of the House Judiciary Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 3405. 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.

CCIA firmly believes that children are entitled to greater security and privacy online. Our members have designed and developed settings and parental tools to individually tailor younger users' online use to their 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 allow parents to block specific sites entirely.[2] This is also why CCIA supports implementing digital citizenship curricula in schools, to not only educate children on proper social media use but also help teach parents how they can use existing mechanisms and tools to protect their children as they see fit.[3]

The proposed language regarding age verification and parental consent requirements for covered manufacturers and developers raises significant concerns. We appreciate the opportunity to expand on those concerns as the Committee considers this proposal. While CCIA shares the goal of increasing online safety, this bill presents the following concerns.

## Currently available tools to conduct age determination are imperfect in estimating users' ages.

Every approach to age determination presents trade-offs, especially between accuracy and privacy. There is also no one-size-fits-all approach as the nature of the content and risks varies widely across online services. Therefore, different services base their approaches on a variety of factors, including but not limited to their user base, the service offered, risk calculation, privacy expectations, and economic feasibility.[4] There are also significant differences and dynamics tied to various levels of conducting age assurance, including attestation, estimation,

[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] Competitive Enterprise Institute, *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/.
[3] Jordan Rodell, *Why Implementing Education is a Logical Starting Point for Children's Safety Online*, Disruptive Competition Project (Feb. 7, 2023), https://project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/.
[4] *Age Assurance: Guiding Principles and Best Practices*, Digital Trust & Safety Partnership (Sept. 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.

and verification.[5] A recent Digital Trust & Safety Partnership (DTSP) report, Age Assurance: Guiding Principles and Best Practices, contains more information regarding guiding principles for age assurance and how companies have used such principles to develop best practices.[6]

The National Institute of Standards and Technology (NIST) recently published a report examining the performance of six software-based age estimation and age verification tools that estimate a person's age based on the physical characteristics evident in a photo of their face.[7] The report notes that facial age estimation accuracy has improved since NIST first measured it in 2014.[8] However, recent research has shown that accuracy is strongly influenced by algorithm, sex, image quality, region-of-birth, age itself, and interactions between those factors; the lowest false positive rates are observed among Eastern Europeans, though these rates vary for women and men of different ages, with false positives generally being higher in women compared to men.[9] While the authors of the report note that improvements to such technologies are anticipated to rapidly evolve and that NIST intends to update and expand their test methods, CCIA encourages lawmakers to consider the current technological limitations in providing reliably accurate age estimation tools across all demographic groups.

## Age verification and parental consent requirements raise significant privacy concerns.

The proposed act suggests imposing a government-mandated requirement to verify all South Carolina users' ages that conflicts with data minimization principles ingrained in standard federal and international privacy and data protection compliance practices. Determining a user's age and verifying parental consent inherently requires collecting additional, sensitive data from those users. If the state were to force companies to collect more user data even as others are requiring the collection of less data, it may place businesses in an untenable position of picking which state's law to comply with, and which to unintentionally violate.[10]

Additionally, age verification solely at the device operating system or application store level overlooks access to websites via desktop or other devices. Numerous applications are designed for use through a browser, which this method does not cover. While it might seem like a comprehensive solution to regulating access to certain content deemed undesirable for younger users, in reality, it falls short of achieving that goal.

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

[5] Khara Boender, *Children and Social Media: Differences and Dynamics Surrounding Age Attestation, Estimation, and Verification*, Disruptive Competition Project (May 10, 2023), https://www.project-disco.org/privacy/children-and-social-media-differences-and-dynamics-surrounding-age-attestation-estimation-and-verification.
[6] *Age Assurance: Guiding Principles and Best Practices*, *supra* note 4.
[7] Kayee Hanaoka et al., *Face Analysis Technology Evaluation: Age Estimation and Verification (NIST IR 8525),* National Institute of Standards and Technology (May 30, 2024*),* https://doi.org/10.6028/NIST.IR.8525.
[8] *Id.* at 1.
[9] *Id.* at 2-6.
[10] 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.

the government does. The study also highlights why it is important to consider the trade-offs associated with age verification and consent proposals that would require the additional collection data; around 89% of Americans are very or somewhat concerned about social media platforms knowing personal information about kids.[11]

Further, 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 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.[12] 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.

## Restricting access to the internet for younger users may deny them entry to supportive online communities that might be unavailable in their local physical location.

The Children's Online Privacy Protection Act (COPPA)[13] and associated rules at the federal level currently regulate how to address users under 13, a bright line that was the 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. Users between 13 and 18 could face a similar fate as the proposal would implement more complex vetting requirements for those under 18.

When businesses are required to deny access to social networking sites or other online resources, this may also unintentionally restrict younger users' 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.

## Age verification 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.[14] After 25 years, age authentication still remains a vexing technical and social challenge.[15]

---

[11] 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/.
[12] *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.
[13] 15 U.S.C. §§ 6501-6506 (1998).
[14] *Reno v. ACLU*, 521 U.S. 844, 855-57, 862 (1997).
[15] Jackie Snow, *Why age verification is so difficult for websites*, Wall St. J. (Feb. 27, 2022), https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728.

Recent state legislation that would implement online parental consent and age verification or estimation measures is currently facing numerous constitutional challenges, and numerous federal judges have placed laws on hold until these challenges can be fully reviewed, including in Arkansas, California, Mississippi, Ohio, Tennessee, Texas, and Utah.[16] CCIA anticipates that forthcoming rulings from the judiciary may be instructive in determining how, or whether, age determination requirements can be tied to granting user access to online speech. CCIA therefore 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.

## Investing sole enforcement authority with the state attorney general and providing a cure period would be beneficial to consumers and businesses alike.

HB 3405 permits consumers to bring legal action against businesses that have been accused of violating new regulations. By creating a new private right of action, the measure would open the doors of South Carolina's courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. Lawsuits prove extremely costly and time-intensive — it is foreseeable that these costs would be passed on to individual consumers in South Carolina, disproportionately impacting smaller businesses and startups across the state. Further, investing sole enforcement authority with the state attorney general allows for the leveraging of technical expertise concerning enforcement authority, placing public interest at the forefront.

CCIA also recommends that the legislation include a cure period of at least 30 days. This would allow for actors operating in good faith to correct an unknowing or technical violation, reserving formal lawsuits and violation penalties for the bad actors that the bill intends to address. It would also focus the government's limited resources on enforcing the law's provisions for those that persist in violations despite being made aware of such alleged violations. Such notice allows consumers to receive injunctive relief, but without the time and expense of bringing a formal suit.

* * * * *

We appreciate the Committee's consideration of these comments and stand ready to provide additional information as the Legislature considers proposals related to technology policy.

Sincerely,

Megan Stokes
State Policy Director
Computer & Communications Industry Association

[16] *See, e.g.*, *NetChoice v. Bonta*, No. 24-cv-07885, 2025 WL 28610 (N.D. Cal. Jan. 2, 2025); *NetChoice v. Bonta*, No. 22-cv-08861, 2024 WL 5264045 (N.D. Cal. Dec. 31, 2024); *NetChoice, LLC v. Reyes*, No. 23-cv-00911, 2024 WL 4135626 (D. Utah Sept. 10, 2024); *NetChoice, LLC v. Fitch*, No. 24-cv-00170, 2024 WL 3276409 (S.D. Miss. July 1, 2024); *NetChoice, LLC v. Yost*, 716 F. Supp. 3d 539 (S.D. Ohio 2024); *NetChoice, LLC v. Griffin*, No. 23-cv-05105, 2023 WL 5660155 (W.D. Ark. Aug. 31, 2023); *Comput. & Commc'ns Indus. Ass'n et al. v. Paxton*, No. 24-cv-00849, 2024 WL 4051786 (W.D. Tex. Aug. 30, 2024).