

September 17, 2025

Georgia Senate

Senate Impact of Social Media and Artificial Intelligence on Children and Platform Privacy

Protection Study Committee

State Capitol

Atlanta, GA 30303

## Re: SR 431 Study

Dear Co-Chairs Harrell and Still:

On behalf of the Computer & Communications Industry Association (CCIA), I write to provide comments for the forthcoming study pursuant to SR 431.<sup>1</sup> CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.<sup>2</sup> Proposed regulations on the interstate provision of digital services therefore can have a significant impact on CCIA members. CCIA and its members have a shared interest in protecting children and giving parents simple but effective tools to provide a safe online environment for their families.

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.<sup>3</sup> 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.<sup>4</sup>

While we share the goal of increasing online safety and privacy, these comments provide some key considerations to ensure effective and balanced approaches. Restrictive regulations like age-appropriate design codes or age verification mandates raise serious constitutional concerns, as opposed to alternatives like promoting digital citizenship education and voluntary parental tools.

### **Federal courts have recently and repeatedly held that laws requiring age verification online violate the First and Fourteenth Amendments.**

In 2004, the U.S. Supreme Court struck down the Child Online Protection Act (COPA),<sup>5</sup> Congress's attempt to criminalize the posting of content deemed "harmful to minors" unless

<sup>1</sup> S.R. 431, 158th Gen. Assem., Reg. Sess. (Ga. 2025).

<sup>2</sup> 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>.

<sup>3</sup> Competitive Enter. Inst., *Children Online Safety Tools*, <https://cei.org/children-online-safety-tools/> (last updated June 10, 2025).

<sup>4</sup> 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/>.

<sup>5</sup> 47 U.S.C. § 231 (1998).

the poster required “use of a credit card” or ‘any other reasonable measures that are feasible under available technology’” to confirm that the viewer was not a minor.<sup>6</sup> The Court reasoned that since “filtering software is a less restrictive alternative” that would allow “childless adults [to] gain access to speech they have a right to see without having to identify themselves or provide their credit card information,”<sup>7</sup> COPA violated the First Amendment.

Recent state legislation requiring age verification for social media sites has also faced numerous successful constitutional challenges. Federal courts in Arkansas and Ohio have held that such laws violate both the First Amendment’s guarantee of free speech and the Fourteenth Amendment’s Due Process Clause. In Arkansas, the court held that “The State does not have the power to prevent children from hearing or saying anything without their parents’ prior consent. Such laws do not enforce parental authority over children’s speech . . . ; they impose *governmental* authority, subject only to a parental veto.”<sup>8</sup>

The Ohio law was also found to violate the Fourteenth Amendment’s Due Process Clause, in part because it exempted the indefinite category of “‘established’ and ‘widely recognized’ media outlets whose ‘primary purpose’ is to ‘report news and current events,’” with the court concluding that “Such capacious and subjective language practically invites arbitrary application of the law.”<sup>9</sup>

Numerous other federal judges have placed similar laws on hold until challenges can be fully reviewed, including in California,<sup>10</sup> Florida,<sup>11</sup> Mississippi,<sup>12</sup> Texas,<sup>13</sup> and Utah.<sup>14</sup> In California, the Ninth Circuit recently issued a temporary stay against a state law with many similar provisions<sup>15</sup> after the District Court found the law to be “content-based on its face”<sup>16</sup> and to “likely fail strict scrutiny.”<sup>17</sup> Chief Judge Walker in the Northern District of Florida recently summarized the consensus view, stating that “like other district courts around the country, this Court simply recognizes that the First Amendment places stringent requirements on the State to avoid substantially burdening speech unless the State can show that doing so is necessary to achieve its significant interests.”<sup>18</sup>

### **An age verification mandate would curtail individuals’ ability to tailor their preferences regarding content and services and violate their privacy.**

Many products, both digital and physical, can have effective child safety features installed on them even if they are primarily designed for adults. For example, automobiles are designed with seats and seatbelts for adult consumers. However, parents can install car seats designed

<sup>6</sup> *Ashcroft v. ACLU (Ashcroft II)*, 542 U.S. 656, 656 (2004).

<sup>7</sup> *Id.* at 657.

<sup>8</sup> *NetChoice v. Griffin*, No. 23-cv-05105, 2025 WL 978607 at \*31 (W.D. Ark. Mar. 31, 2025) (quoting *Brown v. Ent. Merchs. Ass’n*, 564 U.S. 786, 795) (internal quotation marks omitted) (emphasis in original).

<sup>9</sup> *NetChoice v. Yost*, No. 2:24-cv-00047, 2025 WL 1137485 at \*36 (S.D. Ohio Apr. 16, 2025).

<sup>10</sup> 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).

<sup>11</sup> See, e.g., *CCIA v. Uthmeier*, No. 24-cv-438, 2025 WL 1570007 (N.D. Fla. June 3, 2025).

<sup>12</sup> See, e.g., *NetChoice v. Fitch*, No. 24-cv-00170, 2024 WL 3276409 (S.D. Miss. July 1, 2024).

<sup>13</sup> See, e.g., *CCIA v. Paxton*, 747 F. Supp. 3d 1011 (W.D. Tex. 2024).

<sup>14</sup> See, e.g., *NetChoice v. Reyes*, No. 23-cv-00911, 2024 WL 4135626 (D. Utah Sept. 10, 2024).

<sup>15</sup> *NetChoice v. Bonta*, No. 24-cv-07885 (9th Cir. Jan. 28, 2025) (order granting motion for injunctive relief).

<sup>16</sup> *NetChoice v. Bonta*, No. 22-cv-08861, 2025 WL 807961, at \*6 (N.D. Cal. Mar. 13, 2025).

<sup>17</sup> *Id.* at \*14.

<sup>18</sup> *Uthmeier* at \*1.

specifically for children's safety. Likewise, many devices and services have content filtering technologies that allow parents to individually tailor settings and preferences to select age-appropriate content for themselves and their children. These types of filters and settings, however, are not activated by default.

Even well-meaning proposals often require individuals to share personal information with third parties, including IDs or biometrics, making any holder or processor of the information a prime target for cyberattacks or data breaches.<sup>19</sup> To comply with such requirements, companies are required to collect sensitive identification information that they normally would not, and government officials could access this sensitive data through enforcement inquiries and processes. The collection of detailed personal information about children—and adults—creates massive data pools that criminals will attempt to target for purposes of identity theft.

As explained above, CCIA believes that an alternative to solving these complex issues is to offer more targeted protections, including parental controls, filtering tools, and media literacy education. By working with businesses to continue their ongoing private efforts to implement safety and security mechanisms, the state can provide greater flexibility for families and service providers alike, and better safeguard free speech and privacy.

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

There is no perfect method of age determination, and the more data a method collects, the greater risk it poses to consumer privacy<sup>20</sup> and small business sustainability.<sup>21</sup> 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 digital services have used such principles to develop best practices.<sup>22</sup> The report found that “smaller companies may not be able to sustain their business” if forced to implement costly age verification or assurance methods, and that “[h]ighly accurate age assurance methods may depend on collection of new personal data such as facial imagery or government-issued ID.”<sup>23</sup>

Additionally, age assurance software does not process all populations with equal accuracy. The National Institute of Standards and Technology (NIST) recently published a report evaluating 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.<sup>24</sup> The report notes that facial age estimation accuracy is strongly influenced by algorithm, sex, image quality, region-of-birth, age itself, and interactions between those factors, with false positive rates varying across demographics, generally being higher in women compared to men. CCIA

<sup>19</sup> *Age-verification legislation discourages data minimization, even when legislators don't intend that*, R St. Inst. (May 24, 2023), <https://www.rstreet.org/commentary/age-verification-legislation-discourages-data-minimization-even-when-legislators-don-t-intend-that/>.

<sup>20</sup> Kate Ruane, *CDT Files Brief in NetChoice v. Bonta Highlighting Age Verification Technology Risks* (Feb. 10, 2025), <https://cdt.org/insights/cdt-files-brief-in-netchoice-v-bonta-highlighting-age-verification-technology-risks/>.

<sup>21</sup> Engine, *More Than Just a Number: How Determining User Age Impacts Startups* (Feb. 2024), <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/66ad1ff867b7114cc6f16b00/1722621944736/More+Than+Just+A+Number+-+Updated+August+2024.pdf>.

<sup>22</sup> *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](https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf).

<sup>23</sup> *Id.* at 10.

<sup>24</sup> Kayee Hanaoka et al., *Face Analysis Technology Evaluation: Age Estimation and Verification (NIST IR 8525)*, Nat'l Inst. Standards & Tech. (May 30, 2024), <https://doi.org/10.6028/NIST.IR.8525>.

encourages lawmakers to consider the current technological limitations in providing reliably accurate age estimation tools across all demographic groups.

Vague standards and compliance obligations are likely to lock adult users out from valuable information and services they depend upon if they're unable to verify their age. This is because no age verification or estimation mechanism is 100% accurate, and there will always be false positives that impact adult users.

Even in proposals that are not explicitly age verification mandates, to ensure compliance, businesses need to *determine the age of all users* to ensure that they can adhere to the regulations regarding minors. As explained above, this in turn requires using invasive age verification methods that force businesses to collect sensitive personal identifying information about their users.<sup>25</sup>

## **Limiting access to the internet for children curtails their First Amendment right to information accessibility.**

A lack of narrowly tailored definitions could incentivize businesses to simply prohibit minors from using digital services rather than face potential legal action and hefty fines for non-compliance. The First Amendment, including the right to access information, is applicable to teens.<sup>26</sup> Moreover, requiring businesses to deny access to social networking sites or other online resources may also unintentionally restrict children's ability to access and connect with like-minded individuals and communities. For example, children of certain minority groups may not live in an area where they can easily connect with others that represent and relate to their own unique experiences, so an online central meeting place where kids can share their experiences and find support can have positive impacts.<sup>27</sup>

Due to the nuanced ways in which children under the age of 18 use the internet, it is also imperative to appropriately tailor such treatments to respective age groups. For example, if a 16-year-old is conducting research for a school project, it is expected that they would come across, learn from, and discern from a wider array of materials than a 7-year-old on the internet playing video games. Any definition of "child" or "minor" should be a user under the age of 13 to align with the federal Children's Online Privacy Protection Act (COPPA) standard. This would also allow for those over 13, who use the internet much differently than their younger peers, to continue to benefit from its resources.

## **Terms such as "addiction" or "addictive" in an online context lack adequate scientific foundation.**

Humans engage in various compulsive and repetitive behaviors — some of which may negatively impact physical and/or mental health. These could range from binge eating

<sup>25</sup> Berin Szóka, *Comments of TechFreedom In the Matter of Children's Online Privacy Protection Rule Proposed Parental Consent Method; Application of the ESRB Group for Approval of Parental Consent Method*, TechFreedom (Aug. 21, 2023), <https://techfreedom.org/wp-content/uploads/2023/08/Childrens-Online-Privacy-Protection-Rule-Proposed-Parental-Consent-Method.pdf>.

<sup>26</sup> See, e.g., *Reno v. ACLU*, 521 U.S. 844, 874-75 (1997).

<sup>27</sup> *The Importance of Belonging: Developmental Context of Adolescence*, Boston Children's Hospital Digital Wellness Lab (Oct. 2024), <https://digitalwellnesslab.org/research-briefs/young-peoples-sense-of-belonging-online/>.

unhealthy foods to exercising excessively to watching favorite shows for hours on end. However, these behaviors do not necessarily amount to “addictions”. The most recent edition of the *Diagnostic and Statistical Manual of Mental Disorders: Fifth Edition Text Revision (DSM-5-TR)* declined to include definitions for “Internet gaming disorder,” “Internet addiction,” “excessive use of the Internet,” or “excessive use of social media,” noting that “[g]ambling disorder is currently the only non-substance-related disorder included in the *DSM-5-TR* chapter ‘Substance-Related and Addictive Disorders.’”<sup>28</sup>

The connected nature of social media has led some to allege that online services may be negatively impacting teenagers’ mental health. However, researchers explain that this theory is not well supported by existing evidence and repeats a ‘moral panic’ argument frequently associated with new technologies and modes of communication. Instead, social media effects are nuanced,<sup>29</sup> individualized, reciprocal over time, and gender-specific.

Much research on social media and adolescent health (including the National Academies of Sciences, the University of Oxford, the American Psychological Association, and the Journal of Pediatrics) has found that social media does not cause changes in adolescent health at the population level.<sup>30</sup> Even the Surgeon General’s Social Media and Youth Mental Health advisory acknowledges the benefits of social media, including social connection, information sharing, and civic engagement.<sup>31</sup> Indeed, as a federal court recently noted, “nearly all of the research showing any harmful effects” for minors on social media “is based on correlation, not evidence of causation.”<sup>32</sup>

\*

\*

\*

\*

\*

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,

Tom Mann  
State Policy Manager, South  
Computer & Communications Industry Association

<sup>28</sup> Am. Psychiatric Ass’n, *Diagnostic and Statistical Manual of Mental Disorders: Fifth Edition Text Revision* (2022).

<sup>29</sup> Amy Orben et al., Social Media’s Enduring Effect on Adolescent Life Satisfaction, PNAS (May 6, 2019), <https://www.pnas.org/doi/10.1073/pnas.1902058116>.

<sup>30</sup> Regina Park, *The Internet Isn’t Harmful to Your Mental Health, Oxford Study Finds*, Disruptive Competition Project (Jan. 29, 2024), <https://project-disco.org/innovation/the-internet-isnt-harmful-to-your-mental-health-oxford-study-finds/>.

<sup>31</sup> Mike Masnick, *Warning: Believing The Surgeon General’s Social Media Warning May Be Hazardous To Teens’ Health*, Techdirt (June 18, 2024), <https://www.techdirt.com/2024/06/18/warning-believing-the-surgeon-generals-social-media-warning-may-be-hazardous-to-teens-health/>.

<sup>32</sup> *NetChoice v. Yost*, 778 F. Supp. 3d 923, 955 (S.D. Ohio 2025).