April 27, 2026

Louisiana Senate
900 North Third Street
Baton Rouge, LA 70804

Re: HB 134 – "Provides relative to material harmful to minors" (Oppose unless amended)

Dear Chair Miller, Vice Chair Luneau, and Members of the Senate Judiciary Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 134 unless a new definition of the term "minor" that uses an "actual knowledge" standard is added. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] Proposed regulations on the intrastate provision of digital services therefore can have a significant, nationwide impact on CCIA members.

CCIA firmly believes that children are entitled to security and privacy online. Our members have designed and developed 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. However, the bill relies on a definition of "minor" that creates numerous compliance and privacy concerns. Accordingly, CCIA opposes this bill unless this definition is modified.

HB 134 does not define "minor" directly. However, the Louisiana statute referenced for the term "material harmful to minors" defines "minor" as "any person under the age of eighteen years", regardless of whether an interactive computer service collects any information concerning the user's age. Consequently, these services cannot know whether the bill covers their interactions with any given user unless they institute age verification for all users.

This dynamic poses significant privacy concerns: while well-meaning, age verification mandates inherently require collecting sensitive data about users and adults. Such policies run contrary to the data minimization principles underlying federal and international best practices for privacy protection.[3] Requiring individuals to share sensitive personal information with third

[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 Inst., *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/ (last updated June 10, 2025).
[3] *See, e.g.*, *Fair Information Practice Principles (FIPPs)*, Fed. Privacy Council, https://www.fpc.gov/resources/fipps/; *Principle (c): Data Minimisation,* U.K. Info. Comm'r Off.,

parties, including IDs or biometrics, can make recipients a prime target for identity theft, cyberattacks, or other data breaches.[4] Such dangers are far from hypothetical: several of the most devastating data breaches in recent years are directly attributable to age verification requirements.[5] Furthermore, government officials could access this sensitive data through enforcement inquiries and processes. Compounding these problems, the bill requires covered online services to retroactively verify the ages of existing users as well as prospective ones, which unnecessarily increases the risk of malicious actors accessing the data submitted.

The more data a service is forced to collect, the greater risk it poses to consumer privacy and small business sustainability.[6] A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, found that "smaller companies may not be able to sustain their business" if forced to implement costly age verification 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."[7]

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.[8] Though the intention to keep kids safe online is commendable, this bill undermines that initiative by requiring more data collection about young people.

To avoid these issues, CCIA recommends defining the term "minor" (or "known minor") in HB 134 as "*any user of an interactive computer service that the interactive computer service knows to be* under the age of eighteen years."

* * * * *

While we share the concerns of the sponsor and the Committee regarding online youth safety, we encourage Committee members to resist advancing legislation that is not adequately tailored to this objective. We appreciate your consideration of these comments and stand ready to provide additional information as you consider proposals related to technology policy.

---

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/.

[4] Shoshana Weissmann, *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-dont-intend-that/.

[5] *See, e.g.*, Mark Tsagas, *Online Age Checking Is Creating a Treasure Trove of Data for Hackers*, The Conversation (Nov. 11, 2025), https://theconversation.com/online-age-checking-is-creating-a-treasure-trove-of-data-for-hackers-268586.

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

[7] *Age Assurance: Guiding Principles and Best Practices*, DTSP (Sept. 2023) at 10, https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.

[8] *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.

Respectfully submitted,

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