May 15, 2024

Senate Commerce, Consumer Protection and International Affairs Committee
900 North Third Street,
Baton Rouge, LA 70804

RE: HB 577 – "COMMERCIAL REGULATIONS: Prohibits social media companies from collecting data to use for targeted advertising to minors." (Oppose)

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 577 in advance of the Senate Commerce, Consumer Protection and International Affairs Committee hearing on May 15, 2024.

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. Acknowledging policymakers' valid concerns about the online privacy of young individuals, it is imperative to prioritize the establishment of a comprehensive data privacy law applicable to all consumers. This law should incorporate safeguards for sensitive data, specifically addressing information commonly linked to younger users.

CCIA holds a firm conviction that children are entitled to a higher level of security and privacy in their online experiences. Presently, 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] This is also why CCIA supports the implementation of digital citizenship curriculum in schools, to not only educate children on proper social media use but also help educate parents on how they can utilize existing mechanisms and tools to protect their children the way they see fit.[4]

It should also be recognized that protecting children from harm online does not include a generalized power to restrict ideas to which one may be exposed. Speech that is neither obscene to young people nor subject to other legitimate laws cannot be suppressed solely to protect young online users from ideas or images that a legislative body disfavors. Proposals to keep children safe online should be established through a risk-based approach to developing protections for different ages of users and by focusing on tangible harm.

---

[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/.
[4] *See supra* note 2.

Although CCIA did not initially oppose the original language in HB 577, recognizing that many responsible digital services have already implemented measures to safeguard the sensitive personal data of younger users, the supplementary provisions introduced by the House Commerce Committee, mandating age verification for minors and compelling companies to gather further sensitive data on young users, deviate from the bill's original purpose.

CCIA supports enhanced safeguards to protect the personal data of younger users.

The legislative findings of HB 577 recognize the plethora of opportunities and benefits social media has created for children including improved educational experiences. Responsible social media companies have diligently invested substantial efforts to ensure that the online experiences of all users, including children and teens, are not just enjoyable but also appropriate and safe. This is why digital service providers at the device level, application level, and internet service provider (ISP) level have invested, developed, and offered various tools and features to provide additional privacy and security controls for users.[5] As previously mentioned, such measures include default settings around auto-scroll or time limits to help families better manage their child's online environment.

The original text of HB 577 would build upon the work of these companies by prohibiting covered entities from either selling the personal data of minors or using it for targeted advertising. CCIA appreciates lawmakers' efforts to provide additional safeguards for minors but is concerned that such an underinclusive scope would exclude other industries and businesses that pose serious privacy and security risks to younger users.

To avoid leaving younger users unprotected from businesses that fail to adopt standard industry practices, CCIA recommends a few amendments to strengthen the original bill. Although "sensitive personal data" is defined, the term "personal data" is used many times throughout the bill without being defined. CCIA proposes that the definition of "personal data" be narrowed to avoid broadly applying to any type of information. "Personal data" should mean "information that is linked or reasonably able to be linked to an identified or identifiable individual" and "does not include de-identified data or publicly available information."

The term "selling" is also undefined and should be amended to provide covered entities with enough clarity on what practices are prohibited. CCIA suggests that "sale" or "selling" means the exchange of personal data for monetary consideration by a covered entity to a third party. "Selling" should not include the disclosure of personal data (1) to a service provider that processes such information on behalf of the covered entity; (2) as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which that person assumes control of all or part of covered entity's assets; (3) to an affiliate of the covered entity; (4) to a third party for the purposes of providing a product or service requested by the covered user; or (5) the disclosure of personal data that the covered user (a) intentionally made available to the general public via channel of mass media, and (b) did not restrict to a specific audience.

[5] *See supra* note 3.

If these amendments were to be adopted, CCIA believes younger users would not be vulnerable to businesses neglecting to adopt standard industry practices.

The provisions of HB 577 regarding liability for children's data utilization and age verification are unlikely to achieve the bill's stated objectives.

HB 577's newest language contradicts the bill's original intent of discouraging selling the personal data of minors or using it for targeted advertising. Furthermore, this government-mandated requirement is poised to potentially clash with the data minimization principles ingrained in standard federal and international privacy and data protection compliance practices. If the state were to force companies to collect a higher volume of data on users 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.[6]

Additionally, it is important to recognize that age verification solely at the 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 mature adult content, 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 the government does. The study also highlights why it is important to consider the tradeoffs 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.[7]

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.[8] 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.

[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.
[7] 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/.
[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.

Restricting access to the internet for younger users curtails their First Amendment right to information, denying them entry to supportive online communities that might be unavailable in their local physical location.

The Children's Online Privacy Protection Act (COPPA) and associated rules at the federal level currently regulate how to address users under 13, a bright line that was a 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 14 and 17 could face a similar fate as HB 577 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 children's 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.[9] After 25 years, age authentication still remains a vexing technical and social challenge.[10] California, Ohio, and Arkansas recently enacted legislation that would implement online parental consent and age verification requirements — each law is currently facing a legal challenge due to constitutional concerns, and judges recently put all three laws on hold until these challenges can be fully reviewed. The fate of a similar law in Utah is also in jeopardy as it is also facing legal challenges.[11] CCIA 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.

* * * * *

[9] *Reno v. ACLU*, 521 U.S. 844 (1997).
[10] 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.
[11] *NetChoice, LLC v. Bonta* (N.D. Cal. 5:22-cv-08861); *NetChoice, LLC v. Yost* (S.D. Ohio 2:24-cv-00047); *NetChoice, LLC v. Griffin* (W.D. Ark. 5:23-cv-05105); *NetChoice, LLC v. Reyes* (D. Utah 2:23-cv-00911); *Zoulek et al. v. Hass & Reyes* (D. Utah 2:24-cv-00031).

While we share the concerns of the sponsor and the Senate Commerce, Consumer Protection and International Affairs Committee regarding the protection of young people's online data, we encourage Committee members to resist advancing legislation that is not adequately tailored to this objective. 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,

Jordan Rodell
State Policy Manager
Computer & Communications Industry Association