



June 1, 2023

The Office of the Honorable Governor Greg Abbott
P.O. Box 12428
Austin, Texas 78711-2428

RE: HB 18 - “Securing Children Online through Parental Empowerment (SCOPE) Act.” Veto Request

Dear Governor Abbott:

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 regulating what digital services host and how they host it. While recognizing that policymakers are appropriately interested in the digital services that make a growing contribution to the U.S. economy, these bills require study, as they may raise constitutional concerns,² conflict with federal law, and risk impeding digital services companies in their efforts to restrict inappropriate or harmful content on their platforms.

CCIA strongly believes children deserve an enhanced level of security and privacy online. Currently, there are a number of 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.

While CCIA strongly supports the overall goal of keeping children safe online, there are many concerns we would like to raise about the policies this bill would implement, and therefore encourage a veto of HB 18.

1. HB 18's provisions regarding liability for data collection and age verification will not achieve the bill's stated objectives. In fact, the bill may actually put Texans at greater risk of harm, including children that the legislation seeks to protect.

This legislation will inevitably result in companies being required to collect additional information about all users, including adults. This bill provides several examples of how to obtain verifiable consent, however, this raises questions about whether such verification mechanisms would conflict with data minimization principles and other consumer data privacy protection measures. CCIA is concerned that businesses may be forced to collect geolocation and age verification data, which would paradoxically force companies to collect a higher volume of data on users.⁴ Businesses may be forced to accumulate personal information they do not

¹ For over 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 Eric Goldman, *The Constitutionality of Mandating Editorial Transparency*, 73 *Hastings L.J.* 1203 (2022), https://repository.uchastings.edu/cgi/viewcontent.cgi?article=3985&context=hastings_law_journal.

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/>.

⁴ 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>.

want to collect and consumers do not want to give, and that data collection creates extra privacy and security risks for everyone. 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 that they are of age to be using these services. 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 violate.

It is also important to note that currently, there is no “commercially reasonable age verification method.” The various proposals all come with serious privacy and security risks, both to users and digital service providers. France's data protection agency recently evaluated⁵ various age-verification systems and concluded that there is no solution that satisfactorily meets the requirements concerning privacy, security, accuracy, and more.

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.⁶ After 25 years, age authentication still remains a vexing technical and social challenge.⁷ California recently enacted legislation that would implement similar age verification measures which is currently being challenged for similar reasons.⁸ CCIA recommends that lawmakers permit this issue to be more fully examined by the judiciary before burdening businesses with legislation that risks being invalidated.

2. This bill may result in shutting down services for all users under 18, including access to supportive communities that may not be available in their 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 users and 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 18 would implement more complex vetting requirements tied to parental consent for users 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.

Serious concerns also arise when verifying whether a “verified parent” is in fact a 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 “verified parent” is actually a minor's legal parent or guardian, this may incentivize minors to ask other adults

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 *Reno v. ACLU*, 521 U.S. 844 (1997).

⁷ 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>.

⁸ *NetChoice v. Bonta* (N.D. Cal. 22-cv-08861).

that are not their legal parent or guardian to verify their age on behalf of the minor to register for an account with a “digital service provider.” 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 Texas or is not a resident of the state creates significant confusion for consumers and businesses.

An online central meeting place where younger users can share their experiences and find support can have positive impacts. Teens themselves paint a nuanced picture of the effects of social media. It is one in which majorities credit these platforms⁹ with deepening connections and providing a support network when they need it. In a recent survey, 80% of teens say that what they see on social media makes them feel more connected to what’s going on in their friends’ lives, while 71% say it makes them feel like they have a place where they can show their creative side. Additionally, 67% also say these platforms make them feel as if they have people who can support them through tough times.

3. A mandatory device filter would remove a user’s individual ability to tailor preferences regarding content and services.

Mandating that a device activate a “filter” intended to prevent younger users from accessing certain content ignores the fact that adults, by and large, are the primary users of the cellular phone and tablet devices that the bill explicitly seeks to regulate. In the global economy, we use many products and services that are not, by default, designed for younger users. For example, automobiles are designed with seats and seatbelts for adult consumers. However, car seats designed specifically for children’s safety are available and recommended for use to ensure that children are as safe as possible when riding in an automobile. In a similar vein, many devices and services have content filtering technologies that allow parents to individually tailor settings and preferences to enable both adults and children to make appropriate choices about the type of content and services they are able to see and use. These types of filters and settings, however, are not activated by default. HB 18 could invite significant consumer confusion for adults unaware that such filters aimed for children are set by default. CCIA would recommend that the use of such filters continue to be voluntary and an opt-in feature for the specific consumers who wish to utilize them.

Further, HB 18 creates significant liability concerns due to the subjective nature of what may be considered “harmful material or obscene”. Standards for what is deemed to be art versus potentially “obscene” are tied to different community and cultural norms that can vary considerably across small geographic areas. The notion that a device could accurately adapt to these dynamic and subjective norms as it is moved about is implausible and certain to result in over-filtering.

4. Several of the bill’s provisions are extremely broad and may apply to a wide array of services and activities creating significant compliance difficulties.

In order to achieve meaningful children’s safety protections, it is imperative for businesses to have a roadmap of how to properly comply and avoid unintentional violations. This bill provides broad strokes of *what* is expected of businesses but does not portend *how* businesses may achieve those objectives. HB 18 creates difficult compliance requirements that run counter to data minimization principles. Complying with the duty to register the age of a user forces organizations to collect sensitive information about all users, both over and

⁹ Monica Anderson *et al.*, *Connection, creativity and drama: Teen life on social media in 2022*, Pew Research Center: Internet, Science & Tech (Nov. 17, 2022), <https://www.pewresearch.org/internet/2022/11/16/connection-creativity-and-drama-teen-life-on-social-media-in-2022/>.



under 18, to ensure the user is not a minor. This mandate creates serious privacy and security risks for users and businesses alike. This challenge is further compounded by the lack of guidance on what constitutes as a “commercially reasonable age verification method” despite no such thing currently existing.¹⁰ CCIA cautions against conflating concepts regarding age attestation versus age verification.¹¹ For example, when a website asks a user to make a self-attestation of their age, such as on a website for alcohol products, the owner of that website is not held liable if that user chooses to mischaracterize their identity. Similar self-attestation measures are currently in place for social media platforms and other digital services, and the burden is on the consumer to be forthcoming and honest about the age and birth dates they enter. Further, it is unclear what impact the use of VPNs and similar mechanisms to evade age verification by users could have on organizations’ liability under this bill.

The vague “duty to prevent harm to known minors” also creates difficult gray areas for business and would adversely impact the experience of all users. It is unclear whether a user sharing a clip from a popular TV show that includes some content about a school “bully” would constitute a violation of this duty. This vagueness may result in some more cautious websites ceasing to provide forums for user-generated content online due to perceived risk, which will ultimately harm users. For example¹², a user could be leading a discussion about ways to combat eating disorders and their journey to recovery. However, because an eating disorder was mentioned, a digital service provider may be forced to remove this content from their platform due to the possibility that it may constitute a failure to prevent harm. This could result in users (both under 18 and over) losing access to important content around these issues, including group discussions and materials about seeking help and mitigating harm.

* * * * *

While we share the concern regarding the safety of young people online, we encourage policymakers to resist enacting legislation that is not adequately tailored to this objective. We respectfully urge you to veto HB 18. We appreciate your consideration of these comments and stand ready to provide additional information as the legislature considers proposals related to technology policy.

Sincerely,

Khara Boender
State Policy Director
Computer & Communications Industry Association

¹⁰ Emma Roth, *Online age verification is coming, and privacy is on the chopping block*, The Verge (May 15, 2023), <https://www.theverge.com/23721306/online-age-verification-privacy-laws-child-safety> (“As pointed out by CNIL’s report on various online age verification options, all these methods have serious flaws.”).

¹¹ 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/>.

¹² Munmun De Choudhury, *Anorexia on Tumblr: A Characterization Study*, DH '15: Proceedings of the 5th Int’l Conference on Digital Health 2015 (Ass’n for Computing Mach. 2015), <http://www.munmund.net/pubs/dh15.pdf>.