March 22, 2023

Joint Committee on Judiciary
Attn: Kristin Breiner, Committee Administrator
Legislative Office Building
300 Capitol Avenue
Hartford, CT 06106

Re: S.B. 3 - An Act Concerning Online Privacy, Data and Safety Protections and An Employer's Duty to Disclose Known Instances of Sexual Harassment or Assault Committed by An Employee When Making Employment Recommendations.

Dear Co-Chair Winfield, Co-Chair Stafstrom, and Members of the Joint Committee on Judiciary:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully raise a few concerns with S.B. 3, An Act Concerning Online Privacy, Data and Safety Protections and An Employer's Duty to Disclose Known Instances of Sexual Harassment or Assault Committed by An Employee When Making Employment Recommendations.

CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] CCIA supports the enactment of comprehensive federal privacy legislation to promote a trustworthy information ecosystem characterized by clear and consistent consumer privacy rights and responsibilities for organizations that collect and process data. A uniform federal approach to the protection of consumer privacy throughout the economy is necessary to ensure that businesses have regulatory certainty in meeting their compliance obligations and that consumers are able to exercise their rights. CCIA appreciates, however, that in the absence of baseline federal privacy protections, state lawmakers are attempting to fill in the gaps. To inform these efforts, CCIA produced a set of principles to promote fair and accountable data practices.[2]

CCIA strongly supports the protection of consumer data and understands that Connecticut residents are rightfully concerned about the proper safeguarding of their data, particularly when it comes to health information and children's data. However, as currently written, S.B. 3 includes several provisions that raise

[1] For 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] Computer & Communications Industry Association, *Considerations for State Consumer Privacy Legislation: Principles to Promote Fair and Accountable Data Practices* (January, 2022), https://www.ccianet.org/wp-content/uploads/2022/02/CCIA-State-Privacy-Principles.pdf

concerns. We appreciate the committee's consideration of our comments regarding several areas for potential improvement.

Regarding Section 1 of S.B. 3

1. "Consumer health data" should be more narrowly defined and "Personal information" omitted.

While CCIA understands and supports the intent of this section, S.B. 3 defines "consumer health data" so broadly that it would likely include data about daily consumer activities and purchases by including any data related to "bodily functions" and "gender-affirming care information". This broad definition could capture the regular purchase of items such as feminine care products, sexual health products, undergarments, or items as simple as toilet paper. By including routine purchases such as hygienic products within the scope of this legislation, consumers would constantly be required to provide consent in the course of normal transactions. This would inevitably lead to consent fatigue while not actively contributing to accomplishing the legislation's intent.

Furthermore, the language pertaining to location information included in the definition of "consumer health data" should be also narrowed in its scope. CCIA suggests adjusting the language to "precise location information that could reasonably indicate such consumer's *primary purpose is to* attempt to acquire or receive health services or supplies". As currently written, a device would not be able to collect a consumer's current location data to provide them with directions to where they are seeking to go, whether that be home, the nearest grocery store/pharmacy, or otherwise.

In addition, the definition of "personal information" included in the proposed legislation is problematic as companies are already spending resources to comply with a patchwork of privacy laws, including the robust CTPDA. Therefore, the inclusion of a new definition of data - "personal information"- that diverges from these growing obligations is of concern. To avoid further confusion and unnecessary burdens for operators, we recommend removing the definition of personal information until CTPDA goes into effect.

2. Restrictions on the use of geofencing should depend on the consumer's choice to consent.

The current blanket prohibition on the implementation of geofencing around a facility providing health care services ignores certain scenarios where some consumers may want to opt-in to the use of technology that utilizes a geofence. For example, a consumer may want to opt-in to the use of a system that allows them to virtually check-in for a doctor's appointment that becomes available to them when they arrive at a healthcare facility, allowing them to wait outside the facility or in their

vehicle until a health care provider is able to see them. In addition, responsible companies continue to make progress in implementing measures that protect users while providing them with important services.[3] To meet consumers' demand for such services, we suggest that the language be amended to prohibit the implementation of a geofence to identify, track, collect data from or send notifications to a consumer, unless such a consumer opts-in and consents to the use of such technology.

Regarding Section 2 of S.B. 3

1. Any legislation should be sure to avoid unintended pitfalls which could put more children at risk.

As other states have considered well-intended legislation to shape childrens' online experience, many proposals that have been considered would implement requirements that would actually require the harvesting of additional data on all internet users, including children, and would enable third-party verification applications to access childrens' data[4]. By requiring parental consent before allowing a child under sixteen years of age to open a social media account, businesses may be forced to accumulate personal information they don't want to collect and consumers don't want to give, and that data collection creates extra privacy and security risks for everyone, including children. Furthermore, implementing a parental consent requirement would likely require a verification process, and some states have considered measures that would authorize or even mandate the use of a third-party verification application, which would once again require the harvesting of childrens' sensitive data, this time sharing that private information with potentially unvetted and questionable operators, raising security concerns.

2. Restricting access to the internet for children also restricts their access to supportive communities that may not be accessible in their physical location.

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, children of racial or other minority groups may not live in an area where they can easily connect with others that represent and relate to their own unique experiences. An online central meeting place where kids can share their experiences and find support can have positive impacts.

In recent years, several efforts have been made to understand the impact of social media on teenagers. Studies have shown that social media effects are nuanced,[5] small at best, reciprocal over

[3] https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/
[4] https://highschool.latimes.com/troy-high-school/opinion-bark-technologies-the-dangers-of-third-party-trackers-for-children/
[5] 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.

time, and gender-specific. Teens themselves also paint a nuanced picture of the effects of social media. It is one in which majorities credit these platforms[6] 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. Limiting access to social media platforms could ultimately have the unintended consequence of hurting teens by stripping them of a vital connection tool.

3. Operators should be provided with a mechanism to obtain additional time to verify and process consumer requests.

Operators may be tasked with verifying and processing thousands of consumer requests at any given moment and have established extensive processes to ensure that they are fully complying with a consumer's request. As a result of these extensive processes, operators may often require additional time to verify that a consumer's request is being made legitimately and subsequently respond to such request. CCIA suggests that subsection (b) of this section be amended to create a mechanism for operators to extend their timeline to respond to a consumer's request by seven days, provided they provide proper notification to the consumer.

Regarding Section 4 of S.B. 3

1. Different age groups operate differently online and therefore warrant different treatment.

S.B. 3 defines a minor as anyone under the age of 18, but due to the nuanced ways in which children under the age of 18 use the internet, it is 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. We suggest separating out children under the age of 13, who use the internet in a much different fashion, from their older peers to help ensure that older teens can still benefit from the internet's resources, while also ensuring that additional protections are installed for younger internet users.

2. Age verification requirements would lead to the collection of more data from all users, including children.

[6] 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/.

CCIA is concerned that businesses may be forced to collect age verification data, which would paradoxically force companies to collect a higher volume of data on children[7]. Businesses may be forced to collect personal information to track a "minors" activity online, their physical location, and who they communicate with (either to ensure they are a minor or verify that they "allow any adult to contact any minor through any messaging apparatus unless such adult previously established and maintains an ongoing lawful relationship with such minor") in order to comply with the proposed legislation. This puts consumers and businesses in the tough position of sharing and collecting sensitive information that consumers may not want to share, putting in place additional risks for everyone, particularly children and members of other vulnerable communities.

3. Modify the reasonable care duty of controllers to protect the best interests of minors.

As businesses work to bring themselves into compliance with the patchwork of privacy laws pertaining to minors throughout the country, regulatory consistency is important to help avoid confusion. Subsection (a) of Section 4, requires that a controller use reasonable care to avoid any heightened risk of harm to minors proximately caused by such online service, product or feature, which diverts from standards established by other states in their minors privacy laws. Therefore, we suggest creating a definition for "best interests of minors" and amending subsection (a) of Section 4 to require that controller's use reasonable care to protect the best interests of minors, language that has been used in other states. The language we propose is as follows:

To be included in Section 3
"Best interests of minors" means minors' privacy, safety, mental and physical health, access to information, freedom to participate in society, and wellbeing.

To be included in Section 4
"(a) Each controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall use reasonable care to protect the best interests of minors. ~~avoid any heightened risk of harm to minors proximately caused by such online service, product or feature."~~

4. Businesses operating online depend on clear regulatory certainty across jurisdictions nationwide.

[7] 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.

Existing U.S. law provides websites and online businesses with legal and regulatory certainty that they will not be held liable for third-party content and conduct. By limiting the liability of digital services for misconduct by third-party users, U.S. law has created a robust internet ecosystem where commerce, innovation, and free expression thrive — all while enabling providers to take creative and aggressive steps to fight online abuse. Ambiguous and inconsistent regulation at the state level would undermine this business certainty and deter new entrants, harming competition and consumers. This particularly applies to new small businesses that tend to operate with more limited resources and could be constrained by costs associated with compliance. While larger companies may be able to more easily absorb such costs, it could disproportionately prevent new smaller start-ups from entering the market.

Further, careful consideration of what constitutes best practice should involve conversations with practitioners and relevant stakeholders. Online businesses are already taking steps to ensure a safer and more trustworthy internet — recently, leading online businesses announced[8] that they have been voluntarily participating in the Digital Trust & Safety Partnership (DTSP) to develop and implement best practices and recently reported on the efforts to implement these commitments.[9] We urge lawmakers to study both the benefits and drawbacks of teen safety and age verification products and to engage with practitioners and stakeholders to support the ongoing development of practicable solutions.

* * * * *

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

Sincerely,
Alexander Spyropoulos
Regional State Policy Manager - Northeast
Computer & Communications Industry Association

[8] Margaret Harding McGill, *Tech giants list principles for handling harmful content*, Axios (Feb. 18, 2021), https://www.axios.com/techgiants-list-principles-for-handling-harmful-content-5c9cfba9-05bc-49ad-846a-baf01abf5976.html.
[9] *See, e.g.*, DTSP, *The Safe Assessments: An Inaugural Evaluation of Trust & Safety Best Practices* (July 2022), https://dtspartnership.org/wp-content/uploads/2022/07/DTSP_Report_Safe_Assessments.pdf (Appendix III: Links to Publicly Available Company Resources), at 37.