June 26, 2023

Senate Banking, Business, Insurance & Technology Committee
411 Legislative Avenue
Dover, DE 19901

RE: HB 154 - "the Delaware Personal Data Privacy Act" (Oppose unless Amended)

Dear Chair Mantzavinos and Members of the Senate Banking, Business, Insurance & Technology Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 154 unless amended to more consistently align with definitions and principles in other existing comprehensive state privacy laws.

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.[1]

CCIA strongly supports the protection of consumer data and understands that Delaware residents are rightfully concerned about the proper safeguarding of their data. We appreciate the opportunity to expand on several concerns about the provisions included in HB 154.

Modifying several key definitions and provisions to align with existing state privacy laws would facilitate business compliance efforts and consumer understanding of their data privacy rights.

Existing broad-based privacy laws typically recognize a core set of rights and protections including individual control, transparency of processing activities, and limitations on third-party disclosures. However, even minor statutory divergences between frameworks for key definitions or the scope of privacy obligations can create onerous costs for covered organizations. Therefore, CCIA recommends that any consumer privacy legislation is reasonably aligned with existing definitions and rights in other jurisdictions' privacy laws so as to avoid unnecessary costs to Delaware businesses. Alignment of key definitions allows businesses to better practically operationalizable privacy protections across state borders.

[1] 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

To that end, we would suggest that the timeframe for a business to cease processing data be at least 45 days, as specified in most other states. CCIA would also suggest that lawmakers continue to allow covered entities to still be able to process data for internal operations – no other state has prohibited such activity and doing so allows businesses to continue to use such data to improve and repair products and correct technical issues, ultimately leading to consumer benefits. A business should not be vicariously liable for the activities of a business partner who violates contracts. All other states avoid creating this liability. To align with the approach in all other states and avoid introducing unnecessary risk, CCIA recommends amending the language so that liability could be limited to only those situations where there is actual knowledge of a violation.

Regarding consumer data rights, the language should be amended to further align with other states and avoid unnecessary controller obligations. CCIA urges removing the obligation to disclose to consumers a list of the specific third parties to whom a covered organization disclosed the consumer's personal data. CCIA recommends amending the requirement for a controller to specify and detail why it denied an opt-out request for being fraudulent. It creates an unnecessary organizational risk to a business by mandating the disclosure of potential security measures it used to flag fraudulent behavior, while providing little to no benefit to consumers.

CCIA also recommends attention to the following key definitions and would recommend aligning such terms with those specified in recently enacted laws in Connecticut, Iowa, and Virginia: "deidentified data", "sensitive data", and "genetic or biometric data".

CCIA recommends aligning data protection assessment requirements with existing state frameworks.

Data protection assessment requirements in existing state privacy laws are currently consistent across state borders. CCIA encourages lawmakers to model Delaware's data protection assessment provisions in a similar manner. Further, ensuring that this provision applies to all controllers covered by HB 154 would facilitate compliance efforts as covered entities would be more easily able to understand whether they fall within the scope for all provisions of the bill instead of having to determine which specific sections might apply to them. It would also be beneficial to ensure these assessments are provided with attorney-client and work product privilege protections.

CCIA is concerned that HB 154's provisions regarding enhanced children's protections may paradoxically require companies to collect more data about younger users.

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.[2] CCIA's members have been leading the effort in raising 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.

[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/.

As currently written, the bill would create additional protections for all users under 18. Due to the nuanced ways in which users under the age of 18 use the internet, it is imperative to appropriately tailor such treatments to respective age groups. For example, if a 17-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. CCIA suggests limiting such protections to users under 16 to allow older teenage users who use the internet much differently than their younger peers, to continue to benefit from its resources.

To determine when such enhanced protections would be necessary and in light of the bill's willful disregard standard, businesses would need to be able to estimate or verify the age of their users. To achieve compliance and avoid the proposed penalties for violations, it is likely that age estimation would amount to age verification. Such verification requirements raise questions about potential conflicts with data minimization principles and other consumer data privacy protection measures. 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.[3] Businesses may be forced to collect 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.

When the Communications Decency Act was passed, there was an effort to sort the online population into kids and adults for different regulatory treatment. That requirement was struck down as unconstitutional because of the infeasibility. Yet, after 25 years, age authentication still remains a vexing technical and social challenge.[4] 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.

CCIA recommends that any right to cure not be subject to specific criteria and be universally available.

CCIA commends lawmakers for including a cure period but recommends that such a provision not be at the discretion of the attorney general's office and be uniformly applied. No other state privacy law includes criteria for when a right to cure is granted by the Attorney General. A cure period allows for actors operating in good faith to correct an unknowing or technical violation, reserving formal lawsuits and violation penalties for the bad actors that the bill intends to address. This would also focus the government's limited resources on enforcing the law's provisions for those that persist in violations despite being made aware of such alleged violations. Such notice allows consumers to receive injunctive relief, but without the time and expense of bringing a formal suit. Businesses would also be better equipped with the time and resources to address potential privacy changes rather than shifting focus to defending against litigation.

* * * * *

We appreciate your consideration of these comments and stand ready to provide additional information as the legislature considers proposals related to technology policy.

[3] 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.
[4] 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.

Sincerely,

Khara Boender
State Policy Director
Computer & Communications Industry Association