May 17, 2023

Assembly Committee on Commerce and Labor
Room 4100, Legislative Building
401 South Carson Street
Carson City, NV 89701

Re: SB 370 - "Revises provisions relating to the protection of consumer information" - (Oppose).

Dear Chair Marzola and Members of the Assembly Committee on Commerce and Labor:

On behalf of the Computer & Communications Industry Association (CCIA)[1], I write to respectfully oppose SB 370 - "Revises provisions relating to the protection of consumer information".

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 Nevada residents are rightfully concerned about the proper safeguarding of their data, including health and biometric data. However, as currently written SB 370 includes several provisions that raise concerns.

Notably, SB 370 appears to adopt several provisions similar to those included in Illinois' Biometric Information Privacy Act (BIPA). Enacted in 2008, BIPA has been increasingly cited as problematic, particularly with regard to its potential detrimental impact to businesses, given the law's significant fees associated with violations and private right of action.[3] And, a recent Chamber of Progress report revealed several other alarming findings that indicate the law has not been successful in providing consistent and meaningful consumer benefits to consumers. On the contrary, it appears BIPA has resulted in benefiting plaintiff lawyers, and primarily only four main firms – each of those four firms made more than $30 million each from consumer-oriented settlements alone. 88% of BIPA lawsuits have been employer-employee disputes resulting from biometric timekeeping. In the eight BIPA case settlements involving alleged harm to consumers, plaintiffs' lawyers received an average settlement of

[1] CCIA is an international, not-for-profit trade association representing small, medium, and large communications and technology firms. For over 50 years, CCIA has promoted open markets, open systems, and open networks. For more information about CCIA please see: https://www.ccianet.org/about.

[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

[3] Fredric D. Bellamy and Ashley N. Fernandez, *Illinois court decisions acknowledge biometric privacy act's damages a potential business killer,* Reuters (April 17, 2023). https://www.reuters.com/legal/legalindustry/illinois-court-decisions-acknowledge-biometric-privacy-acts-damages-potential-2023-04-17/.

$11.5 million per firm per case, while individuals received an average settlement of $506 per case. We encourage Nevada lawmakers to resist advancing legislation that would have similar results.[4]

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

Definitions should be clear and interoperable.

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 encourages 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 Nevada businesses. As drafted, key definitions in SB 370 are likely to prompt significant statutory interpretation and compliance difficulties, even for businesses with existing familiarity with other US state laws. Specifically, CCIA recommends attention to the recently enacted Virginia Consumer Data Protection Act, along with other states like Utah and Iowa, and alignment of key definitions to allow businesses to better practically operationalizable privacy protections across state borders.

CCIA recommends more-narrowly tailoring several definitions.

CCIA recommends further tailoring the definition of "consumer health data" to ensure that the definition adopts a risk-based approach by providing heightened protections and consumer rights over such information for the most sensitive data – in this, data that is linkable to a specific consumer and that is used to identify the health of a consumer.

This narrower definition would benefit both covered entities and consumers alike. For businesses working toward compliance, this would allow regulated entities to target consent requests from consumers to data definitively within a health-related context and also avoid creating liability for instances outside the bill's intended scope. Relatedly, this would also ensure that consumers would not receive an unreasonable number of opt-in consent notifications in the course of normal transactions. This would inevitably lead to consent fatigue while not actively contributing to accomplishing the legislation's intent.

CCIA recommends considering amendments to narrow the definition of "biometric data". Specifically, the term should mean data which is generated by automatic measurements of an individual's biological characteristics such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify the specific person. The listed inclusions should also be narrowed and clarify that biometric data does not include a digital or physical photograph, an audio or video recording; or any data generated from either unless such data is generated to identify a specific person. This exclusion should also be applied to the term for "biometric identifiers" as used in Sec. 34.3.

Furthermore, the definition of "share" as included in Section 34.4 should align with the exceptions that are included in other privacy laws. CCIA suggests that "share" not include the following: (i) disclosure

[4] Chamber of Progress, *Who Benefits from BIPA: An Analysis of Cases Brought Under Illinois' State Biometrics Law* (April 2023), https://progresschamber.org/wp-content/uploads/2023/03/Who-Benefits-from-BIPA-Analysis-of-Cases-Under-IL-Biometrics-Law.pdf.

of biometric identifiers to a third party when it is considered as part of a merger, acquisition, bankruptcy, or other transaction in which another third party assumes control of all or part of a person's assets; (ii) by a person to a processor that processes the biometric identifiers on behalf of a person; (iii) to a third party for purposes of providing a product or service requested by the consumer; (iv) the disclosure or transfer of a biometric identifier to an affiliate of the person; (v) where the consumer directs the person to disclose the biometric identifier or intentionally uses the person to interact with a third party; or (vi) that the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience.

Further clarity is needed for businesses to appropriately and understand requirements for collecting biometric identifiers.

Many companies use biometric identifiers to strengthen user security, and to combat fraud and illegal activity. These mechanisms help to protect consumers from bad actors and identity theft. Companies also use data for authentication purposes to help verify that the user of a device is in fact the intended user. CCIA suggests amending the language in Sec. 34.5 to ensure entities can process biometric identifiers to prevent, detect, protect against, or respond to security incidents, fraud, harassment, malicious or deceptive activities or any illegal activity; preserving the integrity or security of systems, or investigating, reporting, or prosecuting those responsible for any such action. The amendment could also extend to biometric identifiers used by consumers for purely personal or household activities, ensuring consumers continue to benefit from these technologies.

To that end, CCIA requests further clarification regarding provisions related to biometric identifiers, particularly in Sec. 34.8. The section would require a covered business, before collecting a biometric identifier, to complete the following: (i) inform the user that the biometric identifier is being collected; (ii) specify how long the identifier is being collected, stored, and used, and; (iii) verify the identity of the user, including ensuring that the user for whom the biometric identifier is being collected is present. However, as currently written, this creates significant confusion. If a covered entity is not allowed to collect a biometric identifier before completing the three aforementioned criteria, it is difficult to understand how one could verify that the user is, in fact, present without collecting biometric identifiers. The bill's definition of "biometric identifier"[5] would render it nearly impossible for a covered entity to both receive consent to collect biometric identifier information while confirming the user's identity *without* collecting biometric identifiers. The language in Sec. 30.9 should also be amended to clarify that the sale of a biometric identifier without consent is prohibited, rather than a blanket ban.

* * * * *

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

Sincerely,

[5] SB 370 defines "biometric identifier" as "biometric data relating to the face, fingerprint, or iris of a person. The term includes, without limitation, data from a photo identification document that contains the image of the face of a person with sufficient resolution that artificial intelligence or a machine learning algorithm is able to match the data with other biometric data to positively identify the person".

Khara Boender
State Policy Director
Computer & Communications Industry Association

CC: Office of Senate Majority Leader Cannizzaro
Attn: Mykaela Ryan, Legislative Assistant
Room 1222, Legislative Building
401 South Carson Street
Carson City, NV 89701-4747