May 22, 2023

Committee on Judiciary
Attn: Susan Pinette, Committee Clerk
State House
100 State House Station
Augusta, ME 04333

Re: LD 1705 - An Act to Give Consumers Control over Sensitive Personal Data by Requiring Consumer Consent Prior to Collection of Data.

Dear Co-Chair Carney, Co-Chair Moonen, and Members of the Committee on Judiciary:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose LD 1705, An Act to Give Consumers Control over Sensitive Personal Data by Requiring Consumer Consent Prior to Collection of Data.

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 Maine residents are rightfully concerned about the proper safeguarding of their data, particularly when it comes to their biometric information. However, we believe that efforts to protect biometric data would be better suited being incorporated into a comprehensive data privacy bill, similar to S.P. 807 which was recently introduced and does include biometric data under its definition of "sensitive data". CCIA welcomes the opportunity to work

[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

with the Legislature on comprehensive data privacy legislation, and in the interim offers the following comments on LD 1705, several areas of which are of concern.

1. Investing enforcement authority with the state attorney general and providing a cure period would be beneficial to consumers and businesses alike.

LD 1705 permits consumers to bring legal action against companies that have been accused of violating new regulations. By creating a new private right of action, the measure would open the doors of Maine's courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. Lawsuits also prove extremely costly and time-intensive – it is foreseeable that these costs would be passed on to individual consumers in Maine, disproportionately impacting smaller businesses and startups across the state. Additionally, studies have shown that law firms are the primary financial beneficiaries from biometric privacy-related lawsuits, as in the eight case settlements involving alleged harm to consumers in Illinois, plaintiffs' lawyers received an average settlement of $11.5 million per firm per case, while individuals received an average settlement of $506 per case[3]. Furthermore, investing sole enforcement authority with the state attorney general allows for the leveraging of technical expertise concerning enforcement authority, placing public interest at the forefront.

CCIA recommends that the legislation be amended to include a cure period of at least 30 days. This would allow 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.

2. The terms defined in the bill should be amended to promote interoperability with other states.

Several definitions included in LD 1705 should be amended in order to align with privacy laws that are already in place throughout the country. First, the definition of "biometric identifier" should be amended to include language that addresses data generated by the automated measurements of a consumers' biological characteristics, in order to align better with language from Virginia, Colorado, and Washington's laws. Additionally, the "biometric identifier" definition should fully exempt photos

[3]https://progresschamber.org/new-study-exposes-impact-of-illinois-biometric-privacy-law/

and videos, as to match the language included in the laws in the three aforementioned states. Proposed amended language is included below:

"Biometric identifier. "Biometric identifier" means information generated by automatic measurements of an individual's unique biological characteristics, including a voiceprint or imagery of the iris, retina, fingerprint, face or hand, that can be used to identify that individual. "Biometric identifier" does not include:

A. A writing sample or written signature;
B. A photograph or video, ~~except for measurable biological characteristics that can be generated or captured from a photograph or video;~~
C. A biological sample used for valid scientific testing or screening;
D. Demographic information;
E. A tattoo description or a physical description, such as height, weight, hair color or eye color;
F. A donated organ, tissue or other body part, blood or serum stored on behalf of a recipient or potential recipient of a living or cadaveric transplant and obtained or stored by a federally designated organ procurement organization;
G. Health care information, as defined in Title 22, section 1711-C, subsection 1, paragraph E, obtained for health care, as defined in Title 22, section 1711-C, subsection 1, paragraph C;
H. An x-ray, computed tomography, magnetic resonance imaging, positron emission tomography, mammography or other image or film of the human anatomy used to diagnose or treat an illness or other medical condition or to further validate scientific testing or screening; or
I. Information collected, used or disclosed for human subject research"

Additionally, we suggest that the definition of "personal information" be amended to exempt publicly-available information and de-identified data. Both of these types of data are different from the rest of the information this bill seeks to protect, and Colorado and Virginia include similar exemptions in their laws. Proposed amended language is included below:

"Personal information. "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with a particular individual, household or electronic device. It does not include publicly-available information or de-identified data."

Finally, we suggest that the consent requirement not be limited only to written consent given the nature of biometric uses and contexts. In place of the current language, we suggest that the following be included:

"Consent. 'Consent' means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action."

* * * * *

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