June 08, 2020

House Speaker Scott K. Saiki
Hawaii State Capitol
Room 431
415 South Beretania Street
Honolulu, HI 96813

House Majority Leader Della Au Belatti
Hawaii State Capitol
Room 439
415 South Beretania Street
Honolulu, HI 96813

Representative Sylvia Luke
Chair, House Finance Committee
Hawaii State Capitol
Room 306
415 South Beretania Street
Honolulu, HI 96813

Re: HB 2572 (Oppose)

Dear Speaker Saiki, Majority Leader Belatti, and Chairwoman Luke,

On behalf of the hundreds of companies our organizations represent in the technology, communications, media, innovation, payment card, automobile, online security, health care, and retail sectors, as well as more than 500 magazine brands providing content to more than 90% of U.S. citizens in all 50 states, we write to oppose HB 2572, which attempts to amend the state's data breach law, regulate geolocation, and regulate internet browsing activity. HB 2572 contains very costly outlier requirements that are overly broad and do not reflect widely-accepted privacy and data security protocols, and would have significant unintended consequences as outlined below.

It is also important to re-evaluate legislation in a post-COVID-19 environment. The most recent statistics available show that Hawaii currently has a 22% unemployment rate[1] – an order of magnitude larger than when this bill was last considered in February and early March. This is, of course, similar to how the virus has affected the rest of the nation..

Our members, along with local Hawaiian businesses, are heavily focused on stabilizing the economy, transitioning to a remote workforce, implementing new cybersecurity protocols to protect company networks and consumer data, and discovering innovative ways to combat the COVID-19 pandemic. Given the extraordinary measures that businesses across the world are taking to address novel COVID-19 issues, including the privacy and data security measures referenced above, now is not the right time to increase their economic burden by saddling them with first-in-the-nation mandates which are confusingly drafted, inconsistent with existing privacy and data security requirements, and would cost millions of dollars to implement – precious resources that could better be used on facilitating economic recovery.

We would further request that, in preparation for the 2021 legislative session, the business community be afforded greater participation in any task force or study committee that is convened to examine privacy in a post-COVID era.

I. Data Breach Amendments

The primary principle of data breach notification laws is to provide the affected residents with clear, accurate, and comprehensive information about breaches that pose risk to them. In this area of law, uniformity benefits consumers. The greater the uniformity, and the clearer the definition of data elements that trigger a notice requirement, the more efficiently notices can be provided to the affected individuals, regardless of state lines. This uniformity also results in consistency for consumers, who can better understand the impact of the breach notice they receive and have more consistent guidance for how to address a breach.

HB 2572's proposed definition of "Identifier" would make Hawaii a problematic outlier in the data breach statute ecosystem. The definition is unclear, overly broad, and there is nothing like it in any other state statute. It would create consumer confusion because instead of defining identifier as an individual's first initial and last name, or first name and last name, it defines the term as "a common piece of information related specifically to an individual…to identify that individual across technology platforms." Most fundamentally, this type of information, a

[1] https://www.bls.gov/eag/eag.hi.htm

somewhat amorphous range of data elements, such as advertising cookie ID numbers, internet protocol addresses, and mobile advertising identification numbers *cannot be used* in combination with a "specified data element" by fraudsters to commit identity theft or fraud. Instead, the

individual's name is required. It therefore would be counterproductive to replace the term "identifier" for "name" in current law because residents would receive notice in situations that do not create risk.

Additionally, the "Specified data element" definition contains several overbroad provisions. First, unlike all other state breach notice laws, paragraph (1) would require notice of breaches of the last 4 digits or more of social security numbers. The last 4 digits of an SSN is the most common way to redact SSNs *to promote increased security*. In this form, they cannot be used without the rest of the SSN to commit identity theft or fraud. Yet requiring breach notice of redacted SSNs would eliminate the incentive for businesses to protect the data this way.

Second, nearly every other state combines the elements in (4) and (5) (financial account information and information that allows access to an account). This is because on their own, each data element is not enough to cause a Hawaii resident harm. A credit card number without the security code, or an email account without the password, presents limited danger to the consumer and would result in increased, and meaningless, consumer notifications where no threat of identity theft exists.

What is more, paragraph (5) as drafted reaches *any* access code or password to *any* individual account. It would cover passwords for a host of accounts that create no risk to individuals, if breached – for example, passwords for online news sites, streaming video accounts, dry cleaning, supermarket and other retail accounts. The passwords to these accounts create minimal risk of identity theft or fraud. No state requires notice for breaches of these passwords, because they pose no risk, and Hawaii should not do so either.

II. Geolocation Information & Internet Browser Information

The bill also attempts to restrict the use of both geolocation information and internet browser activity in ways that ignore the realities of the modern online ecosystem. The Twenty-First Century Privacy Law Task Force was responsible for evaluating public policy considerations of privacy legislation and parts of this legislation, including internet browser information, was not part of the Task Force's recommendations of information to regulate. Since there was little input by the entities this bill seeks to regulate during that process, we ask that that this bill be tabled

and that the task force hold meetings on this issue and study it further before proceeding with broad and unreasonable regulation of this area.

a. Geolocation Data

Section 4 is broad and ambiguous in a way that is likely to have significant unintended consequences. The Federal Trade Commission's (FTC) 2012 Privacy Framework notes that precise geolocation is sensitive information for which an entity should receive consent before using, and we do not oppose such a requirement. However, any bill attempting to regulate this should be carefully considered.

H. 2572 includes a very broad definition of "sell" that includes any disclosure in exchange for anything of value. The bill requires opt-in consent for all these disclosures – whereas even the California Consumer Privacy Act (CCPA) of 2018 requires only an opt-out and contains many

exceptions not present in H. 2572. By way of example, there is no fraud prevention or cybersecurity exemption, so that fraudsters could refuse to be tracked and avoid triggering red flags in systems that use location as an element that subjects suspicious transactions to closer inspection and identify patterns that help to prevent future unlawful activities. Likewise, services that allow parents to track the movement of their children's phones would likely require opt-in consent of the children.

These problems would ensue due to the use of the CCPA's definition of "sale" – a definition which produces most of CCPA's unintended consequences. Using this definition here with an opt-in consent requirement would cause more extreme unintended consequences. For example, if a consumer requests a transaction that involves the disclosure of location information from a business to its service provider, must the consumer provide express consent to do so? What if the consumer requests such a transaction but does not provide the consent necessary to complete the transaction? The same is true of a host of other location-based services that do not actually involve "sale" of location data, but where there is some form of compensation offered in connection with location data that is used to deliver a service that users seek or expect.

The definition of "geolocation information" is so broad as to include every photograph or video that is captured by a phone and transferred by a photo application to a cloud storage company. It could also include any information that contains a consumer's zip code, which would provide some broad sense of a consumer's location; or information that contains a customer's purchase

history but does not include geolocation information. These types of unintended consequences should be avoided.

Of course, Hawaii is a unique and treasured tourist destination. The Hawaii Tourism Authority estimated that in 2017, nearly 10 million tourists visited. If every tourist took even 5 photos, that would be 50 million photos generated. Subjecting each one of these to enforcement as a result of, for example, a consumer transferring a photograph from a consumer's email account to his or her social media account is likely not what the legislature intends to regulate, but by applying the CCPA's definition of "sale," that is exactly what would occur.

In short, this section raises far-reaching implications, and should be removed from the bill.

b. Internet Browser Information

The second part of section 4 creates similar issues. First, it goes significantly beyond the Obama Administration FTC Privacy Framework, which does not consider browsing history as sensitive information. It would have significant unintended consequences because types of this information are frequently transferred to keep the provision of services free, as well as to detect suspicious and fraudulent activity that harms individuals conducting legitimate online activity.

Similar to the problems created by using the CCPA definition of "sale" with geolocation information, using the definition of "sale" in the context of internet browser information fails to account for the modern online ecosystem. The bill would impose unreasonable and unwarranted obligations before an internet service provider or any other entity could perform functions that consumers expect.

If consumers do not opt in to uses of data that permit companies to develop new products and services, or to sharing of cybersecurity threat information, both businesses and consumers will suffer. Similarly, much of the free news and content that is available online is supported by advertising, which takes place through the exchange of pseudonymous identifiers. This presents little risk to individuals, who may already opt out of the use of their data for most advertising purposes.[2] Requiring consumers to opt in to these low-risk uses of information that are central to

[2] *See*, *e.g.*, Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, 40-44 (2012); CAN-SPAM CITE; Self-Regulatory Principles for Online Behavioral Advertising (July 2009), *available at*: http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf; Network Advertising Initiative Code of Conduct (2018), available at: http://www.networkadvertising.org/sites/default/files/nai_code2018.pdf.

the delivery of online services is likely to adversely affect availability of these free or low cost services that consumers want and enjoy.

In conclusion, HB 2572 contains confusing requirements in much of the bill that are overbroad and do not account for the modern online ecosystem. We would be willing to work with your committees on a better alternative that achieves the same comprehensive goals, but is much simpler and provides clearer and more meaningful consumer benefits.

Respectfully submitted,

Andrew Kingman
General Counsel
State Privacy and Security Coalition

Courtney Jensen
Executive Director | California and the Southwest
TechNet | The Voice of the Innovation Economy

Tammy Cota
Executive Director
Internet Coalition

Emily Emery
Director of Digital Policy
MPA - The Association of Magazine Media

Laura Curtis
Senior Director, State Government Affairs – California & Hawaii
Computing Technology Industry Association (CompTIA)