



DAVID Y. IGE
GOVERNOR

JOSH GREEN
LT. GOVERNOR

**STATE OF HAWAII
OFFICE OF THE DIRECTOR
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS**

335 MERCHANT STREET, ROOM 310
P.O. BOX 541
HONOLULU, HAWAII 96809
Phone Number: 586-2850
Fax Number: 586-2856
cca.hawaii.gov

CATHERINE P. AWAKUNI COLÓN
DIRECTOR

JO ANN M. UCHIDA TAKEUCHI
DEPUTY DIRECTOR

Testimony of the Department of Commerce and Consumer Affairs

**Before the
Senate Committee on Government Operations
Tuesday, February 16, 2021
3:05 p.m.
Via Videoconference**

**On the following measure:
S.B. 1009, RELATING TO PRIVACY**

Chair Moriwaki and Members of the Committee:

My name is Stephen H. Levins, and I am the Executive Director of the Department of Commerce and Consumer Affairs' (Department) Office of Consumer Protection. The Department supports this bill.

The purposes of this bill are to: (1) amend the definition of "personal information" for the purpose of applying modern security breach of personal information law; (2) prohibit the sale of geolocation information and internet browser information without consent; (3) amend provisions relating to electronic eavesdropping law; and (4) prohibit certain manipulated images of individuals.

The Department supports S.B. 1009's expansion of the definition "personal information" in Hawaii Revised Statutes (HRS) chapter 487N because the current definition is obsolete. Businesses that collect or store data digitally have a responsibility to protect information that is sensitive, confidential, or identifiable from access by hackers; these businesses also have a responsibility to prevent the data from being made available to criminals who engage in identity theft. As of 2018, all 50 states have

data breach notification laws that prescribe when consumers must be notified when their “personal information” has been breached. Hawaii’s data breach notification laws were codified in 2006 as HRS chapter 487N, which, in pertinent part, defines “personal information” in relation to when a breach notification is required, and specifies the circumstances in which a business or government agency must notify a consumer that his or her personal information has been breached. Although Hawaii was one of the first states to enact this law, advancements in technology have made identity theft easier than it was 15 years ago. Businesses and government agencies now collect far more information, and bad actors exploit vulnerabilities in computer databases for nefarious purposes and with increased frequency.

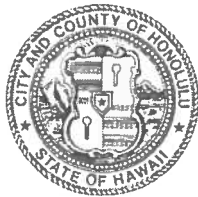
S.B. 1009 corrects existing statutory inadequacies by expanding the definition of “personal information” to include various personal identifiers and data elements, such as email addresses, health insurance policy numbers, security codes, and medical histories. This will enhance consumer protections involving privacy and align with legislation recently enacted in other jurisdictions, including Vermont and California.

With respect to the other elements of S.B. 1009, the Department believes that the bill’s regulation of geolocation data and internet browser information as set forth in part III will advance consumer privacy by prohibiting the sale of consumers’ location data and browsing history without their consent. Lastly, the Department takes no position regarding parts IV and V, since they primarily impact criminal enforcement.

Thank you for the opportunity to testify on this bill.

POLICE DEPARTMENT
CITY AND COUNTY OF HONOLULU

801 SOUTH BERETANIA STREET · HONOLULU, HAWAII 96813
TELEPHONE: (808) 529-3111 · INTERNET: www.honoluluupd.org



RICK BLANGIARDI
MAYOR

SUSAN BALLARD
CHIEF

JOHN D. McCARTHY
AARON TAKASAKI-YOUNG
DEPUTY CHIEFS

OUR REFERENCE **RP-KK**

February 16, 2021

The Honorable Sharon Y. Moriwaki, Chair
and Members
Committee on Government Operations
State Senate
Hawaii State Capitol
415 South Beretania Street, Room 016
Honolulu, Hawaii 96813

Dear Chair Moriwaki and Members:

SUBJECT: Senate Bill No. 1009, Relating to Privacy

I am Captain Randall Platt of the Criminal Investigation Division of the Honolulu Police Department (HPD), City and County of Honolulu.

The HPD opposes Senate Bill No. 1009, Relating to Privacy.

The HPD recognizes the need for the protection of individual privacy rights, especially digital information that can be easily stored, accessed, and transferred. We also hold that there is a legitimate investigative need for law enforcement to be able to access this information to solve crimes. This bill would make it illegal to sell information to third party companies and prohibit the use of public record gathering software such as Citizen Law Enforcement Analysis and Reporting (CLEAR). Software like this allows us to quickly search thousands of data sets to get valuable investigative data. The HPD uses a search warrant to access the stored content, but this bill would require a search warrant for basic subscriber information such as an Internet Protocol or e-mail address or a telephone number.

The HPD urges you to oppose Senate Bill No. 1009, Relating to Privacy, and thanks you for the opportunity to testify.

APPROVED:

Handwritten signature of Susan Ballard in black ink.

Susan Ballard
Chief of Police

Sincerely,

Handwritten signature of Randall Platt in black ink.

Randall Platt, Captain
Criminal Investigation Division

Presentation to The
Committee on Government Operations
February 16, 2021 3:05 p.m.
State Capitol Conference Room 016

Testimony on SB 1009 In Opposition

TO: The Honorable Sharon Y. Moriwaki, Chair
The Honorable Donovan M. Dela Cruz, Vice Chair
Members of the Committees

My name is Neal K. Okabayashi, Executive Director of the Hawaii Bankers Association (HBA). HBA represents eight Hawai`i banks and two banks from the continent with branches in Hawai`i.

HBA does not object to the concept of privacy protection, and in fact, the American Bankers Association testified on December 4, 2019 before a Senate Committee on the ABA's support for a national privacy and data protection measures.

However, it is a difficult task to balance consumer protections and the need for consumer financial transactions in a safe environment, and not hampering innovation that inures to the benefit of consumers.

In Part II, the definition of personal information can be improved by amending the last sentence of the definition of personal information, beginning on page 6, line 21, so that it will read:

“Personal information [does] shall not include publicly available information [that is lawfully made available to the public from federal, state, or local government records, or personal information that is deidentified or aggregated so that the identity the individual is unknown.”

Thus, the last sentence will read as follows: “Personal information shall not include publicly available information, or personal information that is deidentified or aggregated so that the identity the individual is unknown.”

There is no reason that the exception to publicly available information should be restricted to that made available by the government since it could be published in the media, or that it was lawfully available from the government because that would leave the business with the onerous burden of making a legal assessment that it was lawfully available without the facts to make such a determination.

There are also some issues with the proposal redefining personal information, but I defer to the Hawaii Financial Services Association on that issue and support its position.

As to Part III, on geolocation information and internet web browsing, the danger of this provision is that it can be harmful to the consumer because it prohibits the use of such information for use for fraud prevention.

The information on a device may be transferred to a service provider who uses the information to verify the authenticity of the person sending the information to the bank (an identity theft issue) or assesses the fraud risk of the electronic banking application. Only an entity that has received pertinent anti-fraud information from many entities will have enough information to properly assess the fraud and authentication risk, so the information is protective of the consumer's privacy.

Electronic banking has evolved over the years into a service enjoyed by many consumers preferring to do their banking online and in this day of social distancing, more and more customers are choosing to bank digitally. Thus, banks are attempting to accommodate its customers. As new devices get upgraded or innovations are created to protect the consumer's information, the information is embedded in the device and all the device information is transferred to vendors who use the information to prevent fraud.

Part of the problem rests in the very broad definition of sale relating to geolocation and internet browsing so that regardless of purpose, any transfer of such information without consent is a violation.

"Sale" is drafted so that even if the internet browser information or geolocation information were stolen and transferred to a third party, it would still be treated as a sale by the bank of either geolocation information or internet browsing information, because it would be deemed to be a transfer of the information.

One solution is to amend the definition of sale regarding geolocation to read as follows (the proposed amendment is underlined),

"Sale" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a user's geolocation information to another business or a third party for monetary or other valuable consideration. "Sale" shall not include the releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a user's geolocation information for the purpose of responding to an emergency or prevention of fraud.

Similarly, the definition of "sale" regarding internet browser information should be amended to read as follows (the proposed amendment is underlined):

"Sale" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, internet browser information to another business or a third party for monetary or other valuable consideration, except that "sale" shall not include a sale or collection of such information for the purpose of preventing fraud, including using a service provider to collect the information. A service provider is a person or legal entity to which the business discloses or causes the disclosure of personal information, geolocation information, or internet browser information for a business purpose under a written contract, provided that the entity receiving the information shall be prohibited from retaining, using, or disclosing the information for any purpose other than the specific purpose specified in the contract between the service provider and the business.

The simplest solution is to include an exemption in Section 481B- and Section 481B-, exempting financial institutions from those two sections on geolocation information and internet browser information to read as follows:

For a non-bank or savings association financial institution, who is subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102), this part shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act and implementing regulations. Provided further that this part shall not apply to a banks or savings association, as defined in 12 United States Code section 1813, the deposits of which are insured by the Federal Deposit Insurance Corporation, and who are subject to Regulation P, as from time to time amended by the Consumer Financial Protection Bureau or successor department, agency, or bureau, and which bank or savings association's primary supervisory authority is the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, or the Office of the Comptroller of the Currency. “

Although banks and savings associations (banks) are not the only entities subject to GLB, banks are subject to robust and thorough examinations by bank regulatory bodies, which examinations covers compliance, including compliance with privacy laws, Regulation P, and regulations on information technology; all of which are an added layer of protection for consumers. The bank regulatory agencies do not need to await a violation before acting to thwart a potential privacy misstep. The banking agencies can impose severe penalties for unsafe and unsound practices and privacy violations could be an unsafe and unsound practice.

Banks are subject to comprehensive oversight of IT technology as a protective measure against cybersecurity intrusions which may impact privacy. Federal Reserve Chair Jay Powell recently told Congress that cybersecurity is a large risk for banks and other bank regulators have cited cybersecurity as a grave risk.

Reg P is a privacy regulation under the control of the Consumer Financial Protection Bureau, which controls any future amendments thereof. The three banking regulatory agencies have incorporated Reg P into its own regulations. There are other federal privacy statutes such as the Fair Credit Reporting Act (FCRA) and the Right to Financial Privacy Act.

Thus, in the interest of protecting the consumer against fraud and identity theft, HBA opposes the inclusion of the sections on internet browsing and geolocation and desires an amendment to the proposed amendment on personal information.

Thank you for the opportunity to submit this testimony to offer our opposition on SB 1009. Please let us know if we can provide further information.

Neal K. Okabayashi
(808) 524-5161



Testimony of Lisa McCabe
CTIA
In Opposition to Hawaii Senate Bill 1009
Before the Hawaii Senate Committee on Government Operations
February 17, 2021

Chairs, Vice-Chairs, and committee members, on behalf of CTIA®, the trade association for the wireless communications industry, I submit this testimony in opposition to Senate Bill 1009. Definitions in the bill are overly broad, and the legislation would have a host of unintended consequences.

As drafted, the overly broad treatment of the “sale” of “geolocation information” would lead to unintended consequences that could harm—rather than protect—Hawaii consumers. The Federal Trade Commission’s privacy framework considers precise geolocation information as sensitive information. CTIA supports the FTC framework but has concerns with the geolocation section of SB 1009, which could hinder fraud prevention, hamper consumer use of certain applications, and prevent internet companies from providing new and innovative products and services – all to the detriment of consumers. For example, data and artificial intelligence (AI) help providers look for indicators of fraudulent behavior. If a provider sees a consumer logging into an online account from Hawaii, but the consumer’s cell phone is located in New Jersey, that alerts the provider to possible fraud. If a customer’s login occurs from a Hawaii IP address, and the same customer’s cell phone location recently registered in Hawaii, that is a sign the consumer is traveling. A provision requiring a possible



wrongdoer in Hawaii to opt in to the “sale” of location information, which is broadly defined, could hamper a provider’s ability to use location in this way to detect and prevent fraud.

Additionally, there are a number of smartphone apps designed for parents to monitor children, and these are generally based on the use of geolocation information. SB 1009 creates ambiguities for how these apps may function that raise serious concerns. Can children give consent or disable parental controls? Is parental consent sufficient, or could a child override the controls by not giving consent? SB 1009 could ultimately require a child to provide opt-in consent before a parent or guardian can initiate a tracking service or application.

Further, the definition of “geolocation information” is overly broad and will introduce a host of unintended consequences. For example, a consumer’s zip code could be interpreted to fall under the definition of geolocation information, which is not the type of information that CTIA thinks the legislature intends to identify as geolocation information.

Moreover, SB 1009 would only further fragment privacy regulation in the United States. For example, requiring opt-in consent for the “sale” of “internet browser information”—as both terms are broadly defined—deviates from federal guidance. This fragmentation does not benefit consumers.

As the pandemic is still upon us, CTIA respectfully urges the legislature to reject broadly drafted legislation like this bill that could have serious operational impacts and compliance costs. California is the only state to pass comprehensive privacy legislation, and that law comes with estimated initial compliance costs of \$55 billion or 1.8% of the state’s



gross domestic product. For these reasons, CTIA respectfully requests that you not move this legislation.



Charter Communications
Testimony of Felipe Monroig, Senior Director of Government Affairs

COMMITTEE ON GOVERNMENT OPERATIONS

Hawai'i State Capitol
Wednesday, February 16, 2021

OPPOSITION TO S.B. 1009, RELATING TO PRIVACY

Chair Moriwaki, Vice Chair Dela Cruz, and Members of the Committee.

Charter Communications, Inc. ("Charter") is pleased to have this opportunity to provide its views on S.B. 1009. As explained below, Charter supports Hawai'i's efforts to protect the privacy of consumer personal data and give consumers meaningful control of their personal data. While we support the concepts behind the legislation, we oppose enactment of the bill in its current form until certain clarifications are made to address several unintended consequences.

As the largest broadband provider in Hawai'i with services available to over 400,000 homes and businesses in all 4 counties, including Molokai and Lanai, Charter Communications is committed to providing Hawai'i consumers with superior products and services. As a result of significant network investments, Charter's base broadband speed is 200/10Mbps, and we now offer Spectrum Internet Gig (with download speeds of 940 Mbps) across most of Hawai'i. Charter continues to significantly invest in and provide infrastructure improvements, unleashing the power of an advanced, two-way, fully interactive fiber network. By moving to an all-digital network, today's Spectrum customers enjoy more HD channels, more On Demand offerings, more video choices than ever before, and the fastest internet

speeds and the most consistent performance available. Charter offers these services without data caps, modem fees, annual contracts, or early termination fees.

An increasingly important aspect of ensuring that consumers continue to utilize all the services the internet has to offer is making sure they are confident that their personal information is protected. Charter enthusiastically supports such protections, and has taken an active role here and in other forums to promote potential approaches to address the complex issues that impact consumers' online privacy. As Charter has expressed in testimony before the United States Congress and in state houses across the country, an effective privacy framework must be based primarily on five principles.

The first principle is control. Consumers should be empowered to have meaningful choice regarding the collection and use of their data. Any legal framework that is ultimately adopted should ensure consumer consent is purposeful, clear, and meaningful. Additionally, consent should be renewed with reasonable frequency, and any use of personal data should be reasonably limited to what the consumer understood at the time consent was provided. We recognize that there are several policy options as to how to provide consumers with control of their information, and we are willing to work with stakeholders to find practical and impactful solutions.

The second principle is transparency. Consumers should be given the information they need to provide informed consent. Explanations about how companies collect, use and maintain consumers' data should be clear, concise, easy-to-understand, and readily available.

The third principle is parity. Consumers are best served by a uniform framework that is applied consistently across the entire internet ecosystem, not based on who is collecting it or what type of service

is being offered. Consumers' data should be protected equally whether they are using an ISP, a search engine, an e-commerce site, a streaming service, a social network, or a mobile carrier or device.

The fourth principle is uniformity. We believe that for online consumer protections to be effective there should be a single national standard. A patchwork of state laws would be confusing for consumers, difficult for businesses to implement, and hinder continued innovation. However, we realize that in the absence of a uniform, federal solution, some states may consider acting on their own. In doing so, it will be critical that the states understand what each of the others is doing so as to avoid an inconsistent or worse, contradictory, set of online protections.

The final principle is security. We believe privacy is security and security is privacy. Strong data security practices should include administrative, technical, and physical safeguards to protect against unauthorized access to personal data, and ensure that these safeguards keep pace with technological development.

S.B. 1009 contains several problematic provisions, specifically those related to "geolocation information" and "internet browser information." Both of these provisions continue to rely on an outdated and partial definition of "sale" taken from an earlier, and now superseded, version of the CCPA. For example, S.B. 1009 fails to include exceptions for fraud prevention, cybersecurity, internal uses, or deidentified or aggregated information.

Part III of S.B. 1009 also suffers from several additional shortcomings. Part III of S.B. 1009 applies its consent rights to "subscribers," "users," and "primary users," but does not clearly distinguish between those terms or even provide a definition for "primary user." Likewise, the bill mandates that businesses obtain "explicit consent" from consumers, but only provides a definition for "consent," leaving open the

question of whether “explicit consent” is something different. More troubling is that Part III of S.B. 1009, represents legislation for which the Twenty-first Century Privacy Law Task Force, “did not review any specific proposed legislation on the subject.” Part III of SB. 1009 therefore has not been subject to the type of review and consideration that makes for sound, well-reasoned privacy legislation.

These are important issues, and consumers deserve to have the protections envisioned by the task force and the authors of S.B. 1009. But we encourage the legislature to take the additional time necessary to ensure that the provisions of S.B. 1009 are clear to businesses and consumers, and provide sufficient and sustainable privacy protections.

Charter is committed to ensuring that consumer information is protected across the internet ecosystem. That is why, two years ago, our CEO broke new ground by calling for the enactment of federal legislation mandating that all companies receive affirmative, opt-in consent before collecting or sharing their customers’ data. And since that time, Charter representatives have appeared voluntarily and on numerous occasions before lawmakers and policymakers—including Congress and the Federal Trade Commission—to support such a federal privacy law.

Charter looks forward to continuing to work with Members of these Committees, industry partners, consumer groups, and other stakeholders in this process to address the privacy of local residents holistically, sensibly, and effectively through more deliberate legislation.

Mahalo for the opportunity to provide testimony.

STATE PRIVACY & SECURITY COALITION

February 15, 2021

Senator Sharon Y. Moriwaki
Chair, Senate Committee on Government Operations
Hawaii State Capitol, Room 223
Honolulu, HI 96813

Senator Donovan M. Dela Cruz
Vice Chairman, Senate Committee on Government Operations
Hawaii State Capitol, Room 208
Honolulu, HI 96813

Re: SB 1009 (Oppose)

Dear Chairwoman Moriwaki and Vice Chairman Dela Cruz,

The State Privacy & Security Coalition, a coalition of 29 leading telecommunications, technology, retail, payment card, online security, and automobile companies, as well as eight trade associations, writes to oppose SB 1009, which attempts to amend the state's data breach law, regulate geolocation information, and regulate internet browsing activity. This bill would impose significant costs on Hawaii businesses while creating outlier requirements that are overly broad and do not reflect mainstream privacy and data security protocols.

Post-COVID-19, It Is Not the Right Time to Impose Costs on Hawaii Business

As businesses, like the rest of society, attempt to recover from a generational pandemic, this is not the right time to saddle businesses with extraordinary compliance costs. As of December 2020, unemployment in Hawaii stood at 9.0%, with significant challenges facing the accommodation and restaurant sectors.¹ Visitor arrivals are at a fraction of what they were prior to COVID,² and it will take time for the tourist sector to recover. It is appropriate to consider that a study commissioned by the California Attorney General estimated the total cost of compliance with the California Consumer Privacy Act (CCPA) to be \$55 billion, with small and medium-sized businesses expected to spend \$100,000 each on compliance.³ Legislation that diverts resources from hiring, employee safety, and providing consumer services should not be considered at this time.

This bill would likely result in every person in Hawaii repeatedly receiving pop-up opt-in consent notifications similar to the GDPR cookie banners that many of us come across frequently in our internet usage. These are complicated processes to implement and as a result, impose significant costs on the local businesses. Additionally, this bill would require every business in the state to overhaul its privacy policy to reflect the new procedures, adding additional compliance costs.

¹ State economic statistics available at: <http://dbedt.hawaii.gov/economic/>

² *Id.*

³ [Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations](#), Berkeley Economic Advising and Research, LLC, 8-11 (August 2019).

STATE PRIVACY & SECURITY COALITION

SB 1009 is a Costly National Outlier for Hawaii's Economy

Overbroad Definition of "Sale"

This bill is an outlier in a number of ways. First, the bill contains an overbroad definition of sale not found in any state statute, even the CCPA. While it appears similar on its face, it lacks the exemptions to the definition found in CCPA. This would have the effect of creating the broadest definition of "sale" in the nation. Far from regulating a common-sense understanding of what a sale is (the exchange of money in return for a good or service), this definition regulates any transfer of geolocation information to any other entity, even vendors (see below). This has significant effects for any website operated by a Hawaii business, as it regulates the use of cookies which collect geolocation information on website visitors (so that, for example, a small business can know from where its customers are originating). As with the CCPA, any business that employs basic, free cookies which identifies even general location data (since the definition of "precise location" is so broad, as described in section (c), below) to improve services for their customers may be forced to build costly and burdensome opt-in consent mechanisms. As we have also seen with CCPA implementation, doing so will likely confuse customers and give them the impression that the business is engaged in the "sale" of location information, when they are not doing so by any reasonable assessment.

Lack of Service Provider Provisions

Further expanding both the scope and the cost of this bill is the lack of recognition for service providers in the bill. These are companies who have relationships with businesses to perform specific services on behalf of the business, but are generally prohibited from using consumer or resident information for their own uses. Examples of these companies include shipping fulfillment, payment card processing, analytics and first-party marketing, and cloud storage. Because this bill does not recognize this arrangement, literally every transfer of information – even if it is for the business' own purposes and not for an exchange of money – would fall within this bill's scope, creating a regulatory scheme unrecognized in any other state. Even the CCPA – the costliest privacy law ever enacted – recognizes this relationship of business, service provider, and third party.

Overbroad Definition of "Precise Location"

The definition of "Precise location" is overbroad as drafted. The area that the definition proposed covers 3.14 square miles – or just under half the size of Lahaina. In terms of determining location for COVID-19 contact tracing purposes, this is not accurate enough. We would propose a generally accepted definition of 1,750 feet.

Unintended Anti-Privacy Consequences

The bill does not confine itself to Hawaii residents, and thus would apply to any individual located in Hawaii (attempting to expand enforcement beyond this limit would raise significant dormant commerce clause issues). As such, Hawaii businesses would be forced to "geofence" the island, creating notifications when new individuals entered the area, and obtain their consent before providing any services at all. One can imagine this playing out as a tourist arrives at the airport and attempts to contact the hotel for an early check-in via the hotel's app; but before being able to use the app, the tourist must click through a frustrating banner on their phone and scroll through a long privacy policy disclosure.

STATE PRIVACY & SECURITY COALITION

For national businesses, this bill will require that they segregate Hawaii residents from other users, update their privacy policies just for Hawaii, and again impose frustrating opt-in mechanisms on their websites when they are likely not selling geolocation information.

Ironically, SB 1009 as drafted actually requires collecting additional geolocation information to comply, while giving consumers the impression that the business is selling that information.

Internet Browser Information Would Make Hawaii a National Outlier

The second part of section 4 creates similar issues. First, it could have significant unintended consequences for how Hawaii's Internet economy operates. As currently drafted, the bill prohibits the sharing of IP addresses and device identifiers without affirmative consent. This type of information is 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. Such a law could have significant impacts on these most basic operational uses.

Further, the bill goes significantly beyond the Obama Administration FTC Privacy Framework, which does not consider browsing history as sensitive information. The regulation of internet browser information also was not included in the Twenty-First Century Privacy Law Force's recommendations to the legislature. Since the Task Force process contained limited opportunities for input by the entities this bill seeks to regulate, at a minimum, we recommend further task force meetings before proceeding with this type of broad privacy legislation.

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.⁴ Requiring consumers to opt in to these low-risk uses of information that are central to the delivery of online services is likely to adversely affect availability of these free or low cost services that consumers want and enjoy.

Data Breach Amendments Would Frustrate Expedient Consumer Notification

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.

⁴ 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.

STATE PRIVACY & SECURITY COALITION

SB 1009's proposed definition of "Identifier" would make Hawaii a problematic outlier in the data breach statute ecosystem. It 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 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.

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, and in this form, they cannot be used without the rest of the SSN to commit identity theft or fraud. What is more, redaction of SSNs and other sensitive data elements is a good security practice. 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.

We understand the good intentions behind this legislation, but oppose SB 1009 in its current form and believe it should not move forward.

We would be happy to answer any questions and address any concerns you may have.

Respectfully submitted,



Andrew Kingman
General Counsel
State Privacy and Security Coalition



TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet California and the Southwest | Telephone 916.903.8070
915 L Street, Suite 1270, Sacramento, CA 95814
www.technet.org | @TechNetUpdate

February 14, 2021

Senator Sharon Y. Moriwaki
Chair, Senate Committee on Government Operations,
Hawaii State Capitol, Room 223
Honolulu, HI 96813

Senator Donovan M. Dela Cruz
Vice Chairman, Senate Committee on Government Operations
Hawaii State Capitol, Room 208
Honolulu, HI 96813

Re: SB 1009 (Lee) – Privacy Omnibus - Oppose

Dear Chairwoman Moriwaki and Vice Chairman Dela Cruz,

TechNet is the national, bipartisan network of innovation economy CEOs and senior executives. Our diverse membership includes dynamic American businesses ranging from revolutionary start-ups to some of the most recognizable companies in the world. TechNet represents over three million employees and countless customers in the fields of information technology, e-commerce, sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

TechNet respectfully submits this letter in opposition to SB 1009 (Lee), a bill which attempts to amend the state's data breach law, regulate geolocation and internet browser information and regulate internet browsing activity.

In TechNet's previous letter to the 21st Century Privacy Law Task Force, we urged the Task Force not to rush the process of studying and examining appropriate laws and regulations related to privacy. We shared successful models in other states that are thoughtfully studying complicated issues, many of which are included in this bill, and including input from industry and other stakeholders. We have seen the detrimental effect of broad, rushed legislation in states like California, which continues to evolve. Hawaii should not rush to follow. Since that letter, COVID-19 has become a disruption that has altered the economic landscape of Hawaii. SB 1009 would impose significant costs on Hawaiian businesses at precisely the wrong time.

Additionally, there remain extremely broad and overly prescriptive requirements that do not reflect mainstream privacy and data security protocols. As the state privacy landscape evolves, businesses of all sizes and consumers of varying levels of internet facility need understandable guidelines. This legislation contains problematic definitions and requirements for geolocation information and the sale of internet browser

information, both of which will lead to challenging compliance issues. It will overwhelm both constituencies, costing businesses tens of millions of dollars in compliance costs, and confusing consumers. We strongly urge you not to move forward with SB 1009 and work with stakeholders on the breadth of issues this bill is attempting to regulate. TechNet member companies place a high priority on consumer privacy, but moving forward with broad privacy regulation will have a negative impact on business, consumers, and innovation in Hawaii.

For these important reasons, TechNet opposes SB 1009. If you have any questions regarding our opposition to SB 1009 please contact Cameron Demetre, Executive Director, at cdemetre@technet.org or 916-903-8070.

Sincerely,



Cameron Demetre
Executive Director, California and the Southwest
TechNet



**TESTIMONY OF TINA YAMAKI, PRESIDENT
RETAIL MERCHANTS OF HAWAII
February 16, 2021
Re: SB 1009 Relating to Privacy**

Good afternoon Chair Moriwaki and members of the Senate Committee on Government Operations. I am Tina Yamaki, President of the Retail Merchants of Hawaii and I appreciate this opportunity to testify.

The Retail Merchants of Hawaii was founded in 1901, RMH is a statewide, not for profit trade organization committed to the growth and development of the retail industry in Hawaii. Our membership includes small mom & pop stores, large box stores, resellers, luxury retail, department stores, shopping malls, local, national, and international retailers, chains, and everyone in between.

We are opposed to SB 1009 Relating to Privacy as written. This measure amends the definition of "personal information" for the purpose of applying modern security breach of personal information law; prohibits the sale of geolocation information and internet browser information without consent; amends provisions relating to electronic eavesdropping law; and prohibits certain manipulated images of individual.

We would like to point out that it is our understanding that the 21st century privacy law task force created from the House Concurrent Resolution No. 225, Senate Draft 1, Regular Session of 2019, did not have any representation from anyone in the private business community for input or an understanding of our operations. We also acknowledge that California did hastily pass the California Consumer Privacy Act that raised numerous concerns with not only many businesses and but consumers as well regarding the provisions. As a result, California since then has been attempting to correct many the issues.

We are concerned about the broad definition of sale of geolocation information and the definition of sale of internet browser information. It is incredibly open ended and if left up to interpretation could stop most online sales.

Retailers focus is to sell goods and services to our customers. Since the pandemic we have seen a substantial increase in online sales. Customers' expectations of retailers have changed by wanting seamless experience between online and instore shopping and retailers are trying to provide the customer service. Digital mobile technology has enabled retailers to innovate at a greater speed to meet the demands of consumers.

Retailers believe that all businesses handling personal information ought to have direct, statutory obligations to protect that information and honor consumers' rights with respect to it, including processing consumer rights requests. The burden should not fall solely on the consumer-facing companies like retailers to police downstream data use. The mere use of contractual language between retailers and their business partners does not sufficiently hold third parties and service providers accountable for assisting consumer-facing entities, particularly when honoring verified consumer rights requests, or in situations where the retailer is not party to a contract with a downstream vendor. Retailers will often be the first point of contact for customers

about their personal information, but third parties and service providers handling their personal information should have equivalent statutory responsibility for their actions and fulfilling consumer rights requests.

With online sales rising, this measure would hamper retail operations with third party vendors that includes shipping companies, mailing services (FedEx, UPS, US Postal Service) payment processing (credit cards), and warehouses to name a few. Currently retailers take an order online from a customer. If the retailer does not fulfill the order from their site, the fulfillment may go to a third-party warehouse in which the warehouse would need to know the information on who the items are for. The shipper would also be a third-party vendor as the customers address is needed to where the package is shipped to. Retailers like so many other businesses use secure and encrypted cloud storage to maintain information like purchase history (in case there is a return) – which for most businesses would be a third-party vendor.

Retailers support privacy legislation that recognizes that the channel or medium through which customers and businesses interact with each other, including physical locations, must be considered in designing compliant consumer privacy notifications and methods for businesses' secure receipt of consumer rights requests. This would ensure that both the privacy and security of those communications, and the timely processing of customer rights requests, are achieved in the manner most appropriate for each context.

We ask you to hold this measure.

Mahalo again for this opportunity to testify.

HAWAII FINANCIAL SERVICES ASSOCIATION
c/o Marvin S.C. Dang, Attorney-at-Law
P.O. Box 4109
Honolulu, Hawaii 96812-4109
Telephone No.: (808) 521-8521

February 16, 2021

Senator Sharon Y. Moriwaki, Chair
Senator Donovan M. Dela Cruz, Vice Chair
and members of the Senate Committee on Government Operations
Hawaii State Capitol
Honolulu, Hawaii 96813

Re: **S.B. 1099 (Privacy)**
Hearing Date/Time: Tuesday, February 16, 2021, 3:05 p.m.

I am Marvin Dang, the attorney for the **Hawaii Financial Services Association** (“HFSA”). The HFSA is a trade association for Hawaii’s consumer credit industry. Its members include Hawaii financial services loan companies (which make mortgage loans and other loans, and which are regulated by the Hawaii Commissioner of Financial Institutions), mortgage lenders, and financial institutions.

The HFSA **offers comments and a proposed amendment.**

This Bill does the following: (1) amends the definition of "personal information" for the purpose of applying modern security breach of personal information law; (2) prohibits the sale of geolocation information and internet browser information without consent; (3) amends provisions relating to electronic eavesdropping law; and (4) prohibits certain manipulated images of individuals.

In this Bill “personal information”, for the purpose of a security breach of personal information, means an “identifier” in combination with one or more “specified data elements.”

On page 5, line 4 through page 6, line 7 of this Bill is the addition of following definition of “specified data element”:

“Specified data element” means any of the following:

- (1) **An individual's social security number, either in its entirety or the last four or more digits;**
- (2) Driver's license number, federal or state identification card number, or passport number;
- (3) A federal individual taxpayer identification number;
- (4) An individual's financial account number or credit or debit card number;
- (5) A security code, access code, personal identification number, or password that would allow access to an individual's account;
- (6) Health insurance policy number, subscriber identification number, or any other unique number used by a health insurer to identify a person;

...

(bold and yellow highlight added.)

Paragraph 1 of the definition of “specified data element” relates to an individual’s social security number. We agree with intent of the wording in the first phrase of paragraph 1 which includes an individual’s social security number “**in its entirety**” (i.e. the entire 9 digits such as **987-65-4321**) as a specified data element. This is similar to the intent of the other paragraphs of the “specified data element” definition, i.e. a “driver’s license number” (see paragraph 2), a “federal individual taxpayer identification number” (see paragraph 3), an “individual’s financial account number” (see paragraph 4), etc.

That’s also consistent with existing Hawaii statutes which prohibit communicating or making publicly available a person’s entire social security number, i.e. all 9 digits are protected from being displayed.¹

But we disagree with the wording in the second phrase of paragraph 1 in the definition of “specified data element” which includes “**the last four or more digits**” of an individual’s social security number. As the second phrase is written, a “specified data element” would be if the last 4 or more digits was displayed, i.e. **987-65-4321**. That second phrase appears to be repetitive because it encompasses what is already covered by the first phrase (the social security number “in its entirety”) but only in a different way.

We should point out that the usual practice in Hawaii (in the statutes, in the court rules, and for the financial industry) and in other states is to allow shortening, truncating, abbreviating, or limiting the display of an individual’s social security number down to the last 4 digits, i.e. xxx-xx-4321.²

For that reason, we wouldn’t object if paragraph 1 is reworded to include as a “specified data element” **more than** the last 4 digits of a social security number.

Accordingly, we offer two versions of a proposed amendment to this Bill. Under our proposed version #1 below, we recommend that only when the entire 9 digits of the social security number is displayed, that would be a “specified data element”.

Under our proposed version #2 below, we recommend that, separate from displaying the entire 9 digits of the social security number, when more than the last 4 digits is shown, that would be a “specified data element” for the purpose of a security breach of personal information. Thus, displaying more than xxx-xx-4321 would be a “specified data element.”

Below are the two versions:

PROPOSED AMENDMENT - VERSION #1:

“Specified data element” means any of the following:

(1) An individual's social security number, **either in its entirety or the last four or more digits**];

...

¹ See Hawaii Revised Statutes Sec. 487J-2(a)(1) relating to social security number protection. See also the definition of “confidential personal information” in HRS Sec. 708-800.

² Among the Hawaii statutes which require or allow the public display or disclosure of the last 4 digits to be displayed (i.e. xxx-xx-4321) are those where the last 4 digits of an individual’s social security number are displayed when a judgment is to be publicly recorded at the Bureau of Conveyances. See, for example, HRS Secs. 501-151, 502-33, 504-1, and 636-3. Other Hawaii statutes which require redacting or removing the first 5 digits of the social security number so that only the last 4 digits are displayed include HRS Secs. 15-4, 232-7, 232-18, 576D-10.5(f), and 803-6(b).

OR

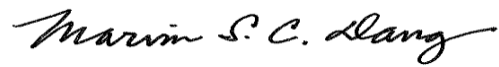
PROPOSED AMENDMENT - VERSION #2:

“Specified data element” means any of the following:

- (1) An individual's social security number, either in its entirety or **more than** the last four **[or more]** digits;

...

Thank you for considering our testimony.



MARVIN S.C. DANG
Attorney for Hawaii Financial Services Association

TESTIMONY OF ALISON UEOKA

COMMITTEE ON GOVERNMENT OPERATIONS
Senator Sharon Y. Moriwaki, Chair
Senator Donovan M. Dela Cruz, Vice Chair

Tuesday, February 16, 2021
3:05 p.m.

SB 1009

Chair Moriwaki, Vice Chair Dela Cruz, and members of the Committee on Government Operations, my name is Alison Ueoka, President of the Hawaii Insurers Council. The Hawaii Insurers Council is a non-profit trade association of property and casualty insurance companies licensed to do business in Hawaii. Member companies underwrite approximately forty percent of all property and casualty insurance premiums in the state.

Hawaii Insurers Council offers three amendments for this Committee's consideration:

First, on page 5, lines 5-6 of the bill, we request that the phrase "either in its entirety or the last four or more digits" be deleted after the phrase "An individual's social security number." Referring to the "social security number" is consistent with existing law, namely, section 487J-2 entitled "Social security number protection," which currently provides that a business or government may not, among other acts, intentionally communicate or otherwise make available to the general public "an individual's entire social security number."

Second, starting on page 6, line 21, through page 7, line 3, the bill recites and makes a minor technical amendment to existing language in section 487N-1, defining what "personal information" does not include. Hawaii Insurers Council requests that page 6, line 21, through page 7, line 3 be amended to read as follows:

"Personal information" [~~does~~] shall not include publicly available information that is lawfully made available to the general public from:

(1) [f]ederal, state, or local government records;

- (2) Widely distributed media; or
- (3) Disclosures to the general public that are required to be made by federal, state or local law.

Exempting from “personal information” publicly available information from widely distributed media reflects the reality that individuals no longer possess a reasonable expectation of privacy in matters that are already in the public domain. Exempting disclosures that are required by federal, state or local law recognizes that businesses need to comply with governmental requirements and orders.

Third, Section 4 of the bill adds two new sections to Chapter 481B, one prohibiting the sale of geolocation information without the primary user’s consent, and the other prohibiting the sale of internet browser information without the internet subscriber’s consent. Hawaii Insurers Council requests that each new section exempt a person providing geolocation information or internet browser information, respectively, to a third-party service provider that performs services for the disclosing person under a contractual agreement for the disclosing person’s business purpose.

Specifically, with respect to geolocation information, we request that section (a) on page 8, lines 9-14 of the bill be amended as follows. Our proposed amendment is indicated by double underscoring:

§481B- Sale of geolocation information without consent is prohibited. (a) No person, in any matter, or by any means, shall sell or offer for sale geolocation information that is recorded or collected through any means by a mobile device or location-based application without the explicit consent of the individual who is the primary user of the device or application. This prohibition shall not apply to a person that sells geolocation information to a third-party service provider performing services for that person under a contractual agreement for that person’s business purposes.

In addition, with respect to internet browser information, we request that section (a) on page 10, lines 6-10 be amended as follows. Our proposed amendment is indicated by double underscoring:

§481B- Sale of internet browser information without consent is prohibited. (a) No person, in any manner, or by any means, shall sell or offer for sale internet browser information without the explicit consent of the subscriber of the internet service. This prohibition shall not apply to a person that sells internet browser information to a third-party service provider performing services for that person under a contractual agreement for that person's business purposes.

Thank you for the opportunity to testify.



To: The Honorable Sharon Y. Moriwaki, Chair
The Honorable Donovan M. Dela Cruz, Vice Chair
Senate Committee on Government Operations

From: Mark Sektnan, Vice President

Re: **SB 1009 – Relating to Privacy**
APCIA POSITION: REQUEST FOR AMENDMENTS

Date: Tuesday, February 16, 2021
3:05 p.m., Conference Room 016

Aloha Chair Moriwaki, Vice Chair Dela Cruz and Members of the Committee:

The American Property Casualty Insurance Association of America (APCIA) is **requesting amendments to SB 1009 related to privacy**. Representing nearly 60 percent of the U.S. property casualty insurance market, the American Property Casualty Insurance Association (APCIA) promotes and protects the viability of private competition for the benefit of consumers and insurers. APCIA represents the broadest cross-section of home, auto, and business insurers of any national trade association. APCIA members represent all sizes, structures, and regions, which protect families, communities, and businesses in the U.S. and across the globe.

APCIA offers three amendments for this Committee’s consideration:

First, on page 5, lines 5-6 of the bill, we request that the phrase “either in its entirety or the last four or more digits” be deleted after the phrase “An individual’s social security number.” Referring to the “social security number” is consistent with existing law, namely, section 487J-2 entitled “Social security number protection,” which currently provides that a business or government may not, among other acts, intentionally communicate or otherwise make available to the general public “an individual’s entire social security number.”

Second, starting on page 6, line 21, through page 7, line 3, the bill recites and makes a minor technical amendment to existing language in section 487N-1, defining what “personal information” does not include. APCIA requests that page 6, line 21, through page 7, line 3 be amended to read as follows:

“Personal information” [does] shall not include publicly available information that is lawfully made available to the general public from:

- (1) [f]ederal, state, or local government records.
- (2) Widely distributed media; or

(3) Disclosures to the general public that are required to be made by federal, state, or local law.

Exempting from “personal information” publicly available information from widely distributed media reflects the reality that individuals no longer possess a reasonable expectation of privacy in matters that are already in the public domain. Exempting disclosures that are required by federal, state, or local law recognizes that businesses need to comply with governmental requirements and orders.

Third, Section 4 of the bill adds two new sections to Chapter 481B, one prohibiting the sale of geolocation information without the primary user’s consent, and the other prohibiting the sale of internet browser information without the internet subscriber’s consent. APCA requests that each new section exempt a person providing geolocation information or internet browser information, respectively, to a third-party service provider that performs services for the disclosing person under a contractual agreement for the disclosing person’s business purpose.

Specifically, with respect to geolocation information, we request that section (a) on page 8, lines 9-14 of the bill be amended as follows. Our proposed amendment is indicated by underscoring:

§481B- Sale of geolocation information without consent is prohibited. (a) No person, in any matter, or by any means, shall sell or offer for sale geolocation information that is recorded or collected through any means by a mobile device or location-based application without the explicit consent of the individual who is the primary user of the device or application. This prohibition shall not apply to a person that sells geolocation information to a third-party service provider performing services for that person under a contractual agreement for that person’s business purposes.

In addition, with respect to internet browser information, we request that section (a) on page 10, lines 6-10 be amended as follows. Our proposed amendment is indicated by underscoring:

§481B- Sale of internet browser information without consent is prohibited. (a) No person, in any manner, or by any means, shall sell or offer for sale internet browser information without the explicit consent of the subscriber of the internet service. This prohibition shall not apply to a person that sells internet browser information to a third-party service provider performing services for that person under a contractual agreement for that person’s business purposes.

For the aforementioned reasons, APCA asks for your favorable consideration of our requested amendments.



Testimony to the Senate Committee on Government Operations
Tuesday, February 16, 2021
3:05 pm
Via Videoconference

Comments on SB 1009, Relating to Privacy

To: The Honorable Sharon Moriwaki, Chair
The Honorable Donovan Dela Cruz, Vice-Chair
Members of the Committees

My name is Stefanie Sakamoto, and I am testifying on behalf of the Hawaii Credit Union League, the local trade association for 51 Hawaii credit unions, representing over 800,000 credit union members across the state.

We offer the following comments regarding SB 1009, Relating to Privacy. This bill amends the definition of "personal information" for the purpose of applying modern security breach of personal information law, and prohibits the sale of geolocation information and internet browser information without consent.

While we understand and agree with the intent of this bill, we suggest amendment for clarification:

With regards to the social security number section of the "specified data element" definition, we would suggest that the definition be expanded to include more than the last four digits. We concur with the amendments proposed by the Hawaii Financial Services Association.

With regards to the geolocation information section, we suggest that language be included that would exclude the sharing of information with service providers, to avoid any service interruption for consumers.

We further concur with the testimony of the Hawaii Bankers Association.

Thank you for the opportunity to provide comments on this issue.

SB-1009

Submitted on: 2/12/2021 3:15:35 PM

Testimony for GVO on 2/16/2021 3:05:00 PM

Submitted By	Organization	Testifier Position	Present at Hearing
lynne matusow	Individual	Support	No

Comments:

We should be required to opt in to all distribution of personal information. Not to have to opt out. I am in full support. This is one of the reasons I refuse to use Facebook.

February 15, 2021

S.B. 1009 Relating to Privacy

Committee: Senate Committee on Government Operations

Hearing Date/Time: Tuesday, February 16, 2021, 3:05 PM

Place: Conference Room 016, State Capitol, 415 South Beretania Street

Dear Chair Moriwaki, Vice Chair Dela Cruz, and members of the Committee:

I write in **support** of S.B. 1009 Relating to Privacy.

As a privacy expert, I have worked in the field of data privacy for over 15 years and am a member of the 21st Century Privacy Law Task Force, created in 2019 by HCR 225.

In 2006, Hawaii passed one of the first data breach notification laws. By 2018, all 50 states have similar laws. Without them, most companies have no obligation to tell consumers when their data is hacked, and we would never have learned of major data breaches like Target and Equifax, affecting over 150 million consumers.

In the last 15 years, the amount of personal information about Americans collected has grown exponentially. In response, most states have updated their data breach notification laws and passed additional privacy legislation. Hawaii should remain in the mainstream by updating our privacy laws, too.

SECTION 2:

The most fundamental part of this bill in the update to the definition of Personal Information in HRS 487-N. Here are several important points relating to the legislation for your consideration:

MEDICAL INFORMATION: Most of us are familiar with HIPAA, a federal law covering medical information held by health care providers and insurance companies. But medical information stored by other companies (like Fitbit or Apple) or apps (like those used for COVID contact tracing) are not subject to HIPAA. Moreover, HIPAA only covers patient data; employee or customer data for *any company* is not covered by HIPAA, this includes COVID test results stored by employers. It falls to state data breach laws to cover (or not) this information. That's why 19 states have already added medical information to their data breach laws (the state names below are hyperlinks to the state laws):

[Alabama](#)
[Arizona](#)
[Arkansas](#)
[California](#)
[Colorado](#)
[Delaware](#)
[Florida](#)
[Illinois](#)
[Michigan](#)
[Missouri](#)

[Montana](#)
[Nevada](#)
[North Dakota](#)
[Oregon](#)
[Rhode Island](#)
[South Dakota](#)
[Texas](#)
[Vermont](#)
[Washington](#)

LAST 4 OF SSN: Hawaii is unique, in that adults born in state have either 575 or 576 as the first 3 digits of their SSN (called the area number). For the next two digits (the group number), Hawaii used as few as 9 two-digit combinations in some years. People who received their SSNs in those years have only 18 possible combinations for the first 5 digits. This makes SSNs very easy to guess if a bad actor has the last 4 digits.

The US government is now starting to recognize the sensitivity of the last digits 4 of the SSN.

- The [IRS](#) defines Personally Identifiable Information in their privacy policy; the enumerated elements list contains “SSN, including the last 4 digits”.
- The [Department of Health and Human Services](#), as part of HIPAA regulations, considers the last 4 of SSN to be identifying information for Protected Health Information.

[AARP](#) sums up the concern for the last for digits of SSN by advising seniors to “Guard the Final Four. Although most widely used and shared, the last four digits are in fact the most important to protect. These are truly random and unique; the first five numbers represent when and where your Social Security card was issued. Scammers can get those numbers by knowing your birth date and hometown. So don’t use the last four as a PIN. Don’t share them in emails. Ask companies to use an alternative identifier.”

ENCRYPTION: HRS 487-N has an exemption to data breach notification in that lost data is not considered a breach if it is encrypted and the encryption key is not compromised. This “safe harbor” is maintained with this bill.

SECTION 4:

GEOLOCATION INFORMATION: As referenced in the bill, the US Supreme Court (in *Carpenter v. United States*) ruled that the government must obtain a warrant to access an individual’s location from their cell phone data. But there is no restrictions on the sale of this information by private companies. Widely publicized dangers include geolocation data being sold to stalkers and bounty hunters.

INTERNET BROWSER HISTORY: The phone company cannot sell a list of the companies you telephone, but internet providers can sell a list of the company websites you visit. The protections should be similar between these two types of common carriers.

Thank you for your consideration and the opportunity support this legislation.

Kelly McCanlies

Kelly McCanlies
Fellow of Information Privacy, CIPP/US, CIPM, CIPT



SB-1009

Submitted on: 2/13/2021 1:16:31 PM

Testimony for GVO on 2/16/2021 3:05:00 PM

Submitted By	Organization	Testifier Position	Present at Hearing
Gerard Silva	Individual	Oppose	No

Comments:

Sounds more like Spying on the people.



February 16, 2021

The Honorable Sharon Y. Moriwaki, Chair
Senate Committee on Government Operations
Hawaii State Capitol
415 South Beretania Street
Honolulu HI 96813

RE: Internet Association Comments on SB 1009

Dear Chair Moriwaki and Members of the Committee:

Internet Association (IA) appreciates the opportunity to provide comments on SB 1009. While IA agrees consumers should have meaningful and easily understood controls over their personal information, we do not believe the proposed legislation is the most effective way to accomplish these goals.

IA represents more than 40 of the world's leading internet companies and advances public policy solutions that foster innovation, promote economic growth, and empower people through the free and open internet.

IA companies know that trust is fundamental to their relationship with consumers. Our member companies recognize that to be successful they must meet consumers' reasonable expectations about how the personal information they provide to companies will be collected, used, and shared. That is why our member companies are committed to transparent data practices, and are continually refining their consumer-facing policies to ensure they are clear, accurate, and easily understood by all consumers.

We have several concerns with the provisions of SB 1009.

Definition of Personal Information

Part II of the legislation should refine the definitions of identifier and personal information. First the definition of an identifier should align with recently introduced privacy legislation (e.g. Virginia Consumer Data Protection Act (VCDPA)) and adopted privacy law (e.g. California Privacy Rights Act (CPRA)) definitions of personal information.

IA would suggest defining an identifier as "*information that is linked or reasonably linkable to an identified or identifiable individual.*" Furthermore, the exemption of publicly available information contained within the definition of personal information is missing key terms for what is considered publicly available information. While the definition exempts information that is lawfully made available to the general public from federal, state, and local government records, it leaves out other types of information that should be considered publicly available. For example, many people post information on public facing websites, which anyone with an internet connection can access. IA believes information people choose to post publicly should not be considered "personal information." Therefore, IA would recommend publicly available information also exempt "*information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person whom the consumer has disclosed the information to, unless the consumer has*



restricted that information to a specific audience” from the definition of personal information. This language is also consistent with the proposed VCDPA and the CPRA.

Sale of Geolocation Information

Additionally, some of the provisions within SB 1009 are overly broad and could cause confusion for consumers and businesses alike. Under Part III, Section 4, the legislation prohibits the sale of geolocation information without explicit consent of the individual who is the primary user of the device or mobile application. First, it is difficult to discern who is the primary user of a device or mobile application located on the device. Oftentimes, there are multiple users of a device due to cost barriers or a device may be transferred from one user to another user making the “primary user” unknown to a covered entity under this legislation. Therefore, we would suggest eliminating “*the primary user of the device or mobile application*” from Section 4 requirements of the bill.

Furthermore, the definitions of geolocation and location-based applications are vague and would have an adverse impact on mobile applications and other services that residents of Hawaii use every day. Instead, IA would suggest that under this Section explicit consent only be required for precise geolocation information that would include “*information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a consumer with precision and accuracy of 1,750 feet, precise geolocation information would not include the contents of the communication or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.*”

We would also recommend there be an exception for sale of precise geolocation information consistent with provisions in CPRA and the proposed VCDPA. This exception would allow businesses to use a consumer’s information when “*necessary to provide a product or service specifically requested by the consumer, perform a contract to which the consumer is a party to, including fulfilling the terms of a written warranty, or take steps at the request of the consumer prior to entering the contract.*” This will allow residents of Hawaii to continue to identify stores, shops, or restaurants nearby; obtain important directions to desired destinations; and receive recommendations on nearby businesses that they may want to visit.

Definition of Consent

IA would also recommend the definition of “consent” for the sale of geolocation information or internet browser history not only be permitted through an opt-in mechanism. Instead, IA would suggest that “consent” be defined as “*a clear affirmative act signifying a consumer’s freely given, specific, informed, and unambiguous agreement to process personal information relating to the consumer. Consent may include a written statement, including a statement by electronic means, or any other unambiguous affirmative action.*” This definition is also consistent with the proposed VCDPA. Currently, SB 1009’s opt-in only method for consent would likely lead to consumers to inadvertently restrict basic uses of their geolocation information or internet browser history, and could result in a frustrated user experience due to the limited functionality of popular internet services. Moreover, this requirement could harm businesses who experience less customer foot traffic as their location and offerings are less easily found online.



Additionally, requiring consumers to provide opt-in consent for every website or every location they visit is cumbersome and will result in people making uninformed choices. As we have seen with the General Data Protection Regulation in the European Union, opt-in consent requests for things like cookies leads to consumers being confused or overwhelmed when accessing the content they have selected. This can result in choices being made out of convenience, rather than evaluating the underlying information and the choices presented. If a consumer visits a website that sells both internet browser history and geolocation information as defined in the bill, they would be required to consider two separate opt-in consent requests for two distinct types of information. As a consequence, this would likely cause the consumer to become frustrated with their online experience being degraded and is unlikely to promote conscientious decision-making regarding the use of their personal information.

Alignment with the Carpenter Decision

While IA does have concerns with other provisions of SB 1009, we are supportive of the inclusion of updated search warrant requirements to align with *Carpenter v. United States*.¹ IA member companies are supportive of state laws being harmonious with federal requirements, especially when it comes to law enforcement access to an individual's information.

IA appreciates the opportunity to explain our initial concerns with SB 1009 and respectfully requests that you hold the bill. We welcome the opportunity to work with you and the committee on these issues going forward. If you have any questions regarding our position, feel free to reach out to me at rose@internetassociation.org or 206-326-0712.

Sincerely,

A handwritten signature in black ink, appearing to read 'Rose Feliciano', with a long horizontal line extending to the right.

Rose Feliciano
Director, Northwest Region, State Government Affairs

¹ 138 S. Ct. 2206 (2018).