

HB2572 HD2

Measure Title: RELATING TO PRIVACY.

Report Title: Privacy; Attorney General; Personal Information; Geolocation Information; Search Warrants; Notice; Deep Fakes

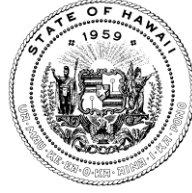
Description: Modernizes "personal information" for the purposes of security breach of personal information law. Prohibits the sale of geolocation information and internet browser information without consent. Amends provisions relating to electronic eavesdropping law. Prohibits certain manipulated images of individuals. Effective 7/1/2050. (HD2)

Companion:

Package: None

Current Referral: CPH/TEC, JDC

Introducer(s): C. LEE



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 Commerce, Consumer Protection, and Health
and
Senate Committee on Technology**

**Tuesday, June 23, 2020
10:00 am
State Capitol, Conference Room 229**

**On the following measure:
H.B. 2572, H.D. 2, Proposed S.D. 1, RELATING TO PRIVACY**

WRITTEN TESTIMONY ONLY

Chair Baker, Chair Keohokalole, and Members of the Committees:

My name is Stephen 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) modernize "personal information" for the purposes of security breach of personal information law; and (2) prohibit the sale of geolocation information without consent.

The Department supports proposed S.D. 1'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of the definition "personal information" in Hawaii Revised Statutes (HRS) chapter 487N because the current definition is obsolete.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 14 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.

Proposed S.D. 1 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.

The Department believes that proposed S.D. 1’s regulation of geolocation data, as set forth in part III, will advance consumer privacy by prohibiting the sale of consumers’ location data without their consent.

Thank you for the opportunity to testify on this bill.

DEPARTMENT OF THE PROSECUTING ATTORNEY
CITY AND COUNTY OF HONOLULU

ALII PLACE
1060 RICHARDS STREET • HONOLULU, HAWAII 96813
PHONE: (808) 768-7400 • FAX: (808) 768-7515

DWIGHT K. NADAMOTO
ACTING PROSECUTING ATTORNEY

LYNN B.K. COSTALES
ACTING FIRST DEPUTY
PROSECUTING ATTORNEY



**THE HONORABLE ROSALYN H. BAKER, CHAIR
SENATE COMMITTEE ON COMMERCE,
CONSUMER PROTECTION AND HEALTH**

**THE HONORABLE JARRETT KEOHOKALO, CHAIR
SENATE COMMITTEE ON TECHNOLOGY
Thirtieth State Legislature
Regular Session of 2020
State of Hawai'i**

June 23, 2020

RE: H.B. 2572, H.D. 2; RELATING TO PRIVACY.

Chair Baker, Chair Keohokalole, Vice-Chair Chang, Vice-Chair English, members of the Senate Committee on Commerce, Consumer Protection and Health and members of the Senate Committee on Technology, the Department of the Prosecuting Attorney, City and County of Honolulu ("Department"), submits the following testimony in support with amendments to H.B. 2572, H.D. 2, Proposed S.D. 1.

The Department would like to first thank the committees for the opportunity to participate as a member of the Twenty-First Century Task Force ("Task Force"). Each member committed an extraordinary amount of time and effort in construction of this bill and our Department would like to commend all the members for their dedication to this important area of law. The current purpose of H.B. 2572, H.D. 2, Proposed S.D. 1 is to ensure further protection for Hawaii residents and their personal data in a digital-focused COVID-19 society by implementing recommendations from the Task Force. The Department believes that the removal of Part IV and Part V from H.B. 2572, H.D. 2 would be contrary to the proposed purpose set out in H.B. 2572, H.D. 2, Proposed S.D. 1 and in *criminal* cases would provide less privacy for Hawaii residents. The Department has outlined below the specific sections of Part IV and V (H.B. 2572, H.D. 2) that the Department believes should be added back into the bill, their application in law and purpose for protecting Hawaii resident's privacy moving forward.

Areas of Amendments:

Part IV, Section 6, Pg. 12 – this section governs law enforcement’s legal authority to compel disclosure of various forms of information stored by “electronic communication services” (such as Google, Apple, Microsoft, Verizon, Hawaiian Telcom, Spectrum, Facebook, and others) and “remote computing services” (such as web hosting companies and cloud-based storage providers like Dropbox). Currently, if law enforcement wants to compel disclosure of the “contents” of communications (such as e-mail, text messages, or private “comments or tweets”), law enforcement must obtain a search warrant. If law enforcement wants to compel disclosure of “transactional records” (such as IP logs, cell site data, and e-mail headers), law enforcement must obtain a court order. If law enforcement wants to compel disclosure of call detail records, or subscriber or account user information, law enforcement is permitted to use a subpoena. The attached proposal eliminates the disparate treatment between “content”, “transactional records”, and account user records, and treats all forms of electronically stored data the same, namely they receive the same protection against disclosure. Thus, if the proposal is adopted, law enforcement would be required to obtain a search warrant (from a neutral judge) before accessing any form of electronically stored data from “electronic communication services” and “remote computing services”, or obtain the consent of the subscriber, customer, or user of the service. **This section is significant, as the proposed amendment will bring Hawaii’s law in line with the 2018 US Supreme Court case of Carpenter v. United States, which held that a search warrant, not a court order, was required to compel access to cell site data.**

Part IV, Section 7, Pg. 16 – this section relates to “court orders” granted at the request of law enforcement that order “electronic communication services” and “remote computing services” to make a “backup” of an online account. Since the proposal to HRS Section 803-47.6 will require that law enforcement obtain a “search warrant” (instead of a “court order”), the proposal to HRS Section 803-47.7 simply replaces the “court order” language with the “search warrant” language.

Part IV, Section 8, Pg. 18 – this section relates to scenarios when the court can delay disclosure to a user. In practice, the court grants delayed disclosure in close to 100% of the cases involving law enforcement’s access to online data. Court-approved non-disclosure orders are based on the need to prevent the harms that are set forth in HRS Section 803-47.8(e). In practice, law enforcement discloses their access to records as part of the discovery process in criminal cases. The discovery materials, including copies of the legal process and records obtained, are provided in discovery to defense counsel and the defendant within 10 days of arraignment, pursuant to Rule 16 of the Hawaii Rules of Penal Procedure (HRPP). The proposal to HRS Section 803-47.8 would retain the judicial discretion provision, and require that disclosure be made no later than the deadline for providing discovery in a criminal case.

Part IV, Section 5, Pg. 12 – This section relates to a proposed amendment to HRS Section 803-41 (the definition section), to update the definition of "electronically stored data". The Task Force agreed that “electronically stored data” would be defined as “any information that is recorded, stored, or maintained in electronic form by an electronic communication service or a remote computing service, and includes, but is not limited to, the contents of communications, transactional records about communications, and records and information that relate to a subscriber, customer, or user of an electronic communication service or a remote computing service.” Thus, it will provide a proper definition for the proposal in Section 803-47.7.

Part V, Section 9, Pg. 20 – this section relates to Hawaii’s Violation of Privacy statute. During the Task Force meetings, the group unanimously approved an amendment that would address the growing problem of “deep fake” videos and images. The Task Force acknowledged that technology

was improving rapidly, and that social media was making it easier to share content. The effects of deep fake technology at the personal and societal level can be devastating and far-reaching. The Task Force recommended that the legislature establish criminal violations for those who violate a person's privacy by creating sexually explicit deep fake videos and images that include their likeness without their consent. Thus, the Task Force unanimously recommended that the legislature adopt Part V to H.B. 2572, which would amend HRS Section 711-111.09.

The Department would note that when this bill was heard in the joint House Committees for Judiciary and Consumer Protection and Commerce, there was no opposition or concerns raised regarding Section IV and V, therefore these section remained intact in H.B. 2572, H.D. 2. Thus, the Prosecuting Attorney of the City and County of Honolulu requests this committee add Section IV and V from H.B. 2572, H.D. 2 into the proposed S.D. 1 to ensure that the privacy rights of Hawaii residents are effectively protected. The Department therefore supports the passage of H.B. 2572, H.D. 2, Proposed S.D. 1 with amendments/additions. Thank you for the opportunity to testify on this matter.



Testimony of
GERARD KEEGAN
CTIA

In Opposition to Hawaii House Bill 2572 SD1

Before the
Hawaii Senate Committee on Commerce, Consumer Protection & Health and Committee on Technology

June 23, 2020

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 House Bill 2572 SD1. Definitions in the bill are overly broad, and the legislation would have a host of unintended consequences.

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 HB 2572 SD1. Data and artificial intelligence (AI) help providers look for indicators of fraudulent behavior. For instance, 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. HB 2572 SD1 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? HB



2572 SD1 could ultimately require a child to provide opt-in consent before a parent or guardian can initiate a tracking service or application. Finally, 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.

In closing, HB 2572 SD1 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. As the pandemic is still upon us, CTIA respectfully urges the legislature to reject hastily 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. Moreover, HB 2572 SD1 would only further fragment privacy regulation in the United States. This fragmentation does not benefit consumers. For these reasons, CTIA respectfully requests that you not move this legislation.



Charter Communications

Testimony of Myoung Oh, Director of Government Affairs

COMMITTEE ON COMMERCE, CONSUMER PROTECTION, AND HEALTH

COMMITTEE ON TECHNOLOGY

Hawai'i State Capitol, Conference Room 229
Tuesday, June 23, 2020
10:00 AM

**OPPOSITION TO H.B. 2572, H.D.2, PROPOSED, S.D.1
RELATING TO PRIVACY**

Chair Baker, Chair Keohokalole, Vice-Chair Chang, Vice-Chair English and Members of the Joint Committees.

Charter Communications, Inc. ("Charter") is pleased to have this opportunity to provide its views on H.B. 2572, H.D.2, Proposed, S.D.1. 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. Charter looks forward to continuing to work with the Committee on Commerce, Consumer Protection and Health, the Committee on Technology, and other stakeholders to achieve those goals. While we acknowledge the changes to the bill since its introduction and 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.

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 supports such protections, and has taken an active role in Hawaii 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 legislatures 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.

CONCERNS WITH H.B. 2572, H.D.2

In our testimony earlier this year before the House Committee on Judiciary and Committee on Consumer Protection, Commerce, and Health, we highlighted our concerns with substantial portions of H.B. 2572, H.D.2, which were derived from an outdated form of the California Consumer Privacy Act of 2018 (the “CCPA”). We appreciate the changes made so far to H.B. 2572, H.D.2 that remove these provisions.

However, H.B. 2572, H.D.2 still 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, H.B. 2572, H.D.2 fails to include exceptions for fraud prevention, cybersecurity, internal uses, or deidentified or aggregated information.

Part III of H.B. 2572, H.D.2 also suffers from several additional shortcomings. Part III of H.B. 2572, H.D.2 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 H.B. 2572, H.D.2 represents legislation for which the Twenty-first Century Privacy Law Task Force, “did not review any specific proposed legislation on the subject.” These are important issues, and consumers deserve to have the protections envisioned by the task force and the authors of H.B. 2572, H.D.2. But we encourage the legislature to take the additional time necessary to ensure that the provisions of H.B. 2572, H.D.2 are clear to businesses and consumers, and provide sufficient and sustainable privacy protections.

CONCLUSION

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.

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.

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.

Thank you again for the opportunity for Charter to present its views.

STATE PRIVACY & SECURITY COALITION

June 22, 2020

Senator Rosalyn Baker
Chair, Senate Committee on Commerce,
Consumer Protection, and Health
Hawaii State Capitol, Room 230
Honolulu, HI 96813

Senator Jarrett Keohokalole
Chair, Senate Committee on Technology
Hawaii State Capitol, Room 203
Honolulu, HI 96813

Re: HB 2572 (Oppose)

Dear Chairwoman Baker and Chairman Keohokalole,

The State Privacy & Security Coalition, a coalition of 30 leading telecommunications, technology, retail, payment card, online security, and automobile companies, as well as eight trade associations, writes to oppose the substitution amendment for HB 2572, which attempts to amend the state's data breach law and regulate geolocation information. Today's substitute purports to address contact tracing in the context of COVID-19, but in reality regulates all types of geolocation information sharing, with costly implications for Hawaii's businesses.

We have also provided amendments with this letter that more directly address the issue of COVID-19 contact tracing.

COVID-19 Legislation Principles

HB 2572 is materially distinct from every other piece of legislation in the country that attempts to regulate COVID-19 contact tracing activities. A contact tracing bill should focus on just that – contact tracing – and should contain the following principles that help safeguard individuals' privacy and make the legislation workable:

- Definition of contact tracing that applies only to precise location and proximity data collected for contact tracing purposes, starting from the date of legislative enactment (allowing for strict segregation between contact tracing data and preexisting data on an individual);
- Individual control (via affirmative consent) on how contact tracing data is used;
- Recognition of vendor/service provider relationships, so that state agencies and private companies can transfer information back and forth for contact tracing purposes, without repeatedly or unnecessarily obtaining consumer consent.
- Recognition that employers and workplaces should not be subject to this type of public health legislation, given the fundamentally different purposes for contact tracing in a larger population and that designed to keep workplaces, customers, and employees safe from COVID-19.

STATE PRIVACY & SECURITY COALITION

- In fact, CDC guidelines recommend that employers conduct daily health checks, and develop a process for notifying employees if they have been exposed to a coworker who has tested positive for COVID-19.¹

While HB 2572 should not, in current form, be considered legislation aimed at a COVID-19 response, we have provided amendments as an addendum to this letter that more precisely targets geolocation information used for contact tracing purposes.

HB 2572 is a Costly National Outlier for Hawaii's Economy

a. 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 California Consumer Privacy Act (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.

b. 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.

c. 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.

¹ CDC's business response guidelines, available at: <https://www.cdc.gov/coronavirus/2019-ncov/community/guidance-business-response.html>

STATE PRIVACY & SECURITY COALITION

d. 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.

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, HB 2572 as drafted actually requires collecting additional geolocation information to comply, while giving consumers the impression that the business is selling that information.

e. Not the Right Time to Impose Costs on Hawaii Business

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.

Now is not the right time to saddle businesses with extraordinary compliance costs. As of April 2020, unemployment stands at 23.5%, a 20.9% increase from April 2019.² Visitor arrivals are down 99.5% in April from last year.³ Businesses and workers are undoubtedly hurting right now, and as our entire nation seeks to define a “new normal” in a COVID-19 era, legislation that hamstring hiring, employee safety, and providing consumer services should not be considered.

We understand the good intentions behind this legislation, but oppose HB 2572 in its current form and believe it should not move forward. Please see our proposed amendments that address the unique issues around contact tracing in the COVID-19 context, which more precisely accords with the stated legislative intent.

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

² State economic statistics available at: <http://dbedt.hawaii.gov/economic/>

³ *Id.*

A BILL FOR AN ACT

RELATING TO PRIVACY.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

PART I

1
2 SECTION 1. The legislature finds that House Concurrent
3 Resolution No. 225 S.D.1, Regular Session of 2019 ("resolution")
4 established the twenty-first century privacy law task force
5 ("task force"), whose membership consisted of individuals in
6 government and the private sector with an interest or expertise
7 in privacy law in the digital era. The resolution found that
8 public use of the internet and related technologies has
9 significantly expanded in recent years, and that a lack of
10 meaningful government regulation has resulted in personal
11 privacy being compromised. Accordingly, the legislature
12 requested that the task force examine and make recommendations
13 regarding existing privacy laws and regulations to protect the
14 privacy interests of the people of Hawaii.

15 The legislature further finds that the task force
16 considered a spectrum of related privacy issues which have been
17 raised in Hawaii and other states in recent years. Numerous

H.B. NO. 2572
H.D. 2
S.D. 1
Proposed

1 states have begun to address the heightened and unique privacy
2 risks that threaten individuals in the digital era of the
3 twenty-first century. Dozens of states have already adopted
4 components of privacy law contained in this Act. California has
5 enacted a comprehensive privacy act, ~~and states such as~~
6 ~~Minnesota, New York, Virginia, and Washington are considering~~
7 ~~comprehensive privacy legislation during their current~~
8 ~~legislative sessions.~~

Commented [KA1]: None of these states passed comprehensive privacy legislation.

9 Following significant inquiry and discussion, the task
10 force made various recommendations on issues such as:
11 modernizing the definition of personal information as it relates
12 to data breaches and the nonconsensual sale of a person's data
13 such as geolocation information.

14 The legislature further finds that in early 2020,
15 governmental and societal responses to the COVID-19 pandemic
16 changed typical types of human interaction. As residents have
17 been mandated and encouraged to stay at home to prevent
18 infection and the spread of COVID-19, an increased online
19 presence has become the new normal. Residents have been forced
20 to use digital methods to shop for groceries and household
21 items, attend classes, complete work projects, and engage in

H.B. NO. 2572
H.D. 2
S.D. 1
Proposed

1 other activity that could usually be done through a non-digital
2 means. Often times these online activities require users to
3 create accounts and share personal information. These online
4 activities also require many businesses to protect a larger
5 volume and new types of data than before, making them potential
6 targets for those looking to steal personal information and data
7 for nefarious purposes.

8 The task force recommended that the definition of "personal
9 information" in chapter 487N, Hawaii Revised Statutes, should be
10 updated and expanded, as the current definition of "personal
11 information" is outdated and needs to be amended. The types of
12 personal information collected by companies online has grown
13 significantly since chapter 487N, Hawaii Revised Statutes, was
14 enacted, and the ways that bad actors can use that information
15 has grown as well. There are many identifying data elements
16 that, when exposed to the public in a data breach, place an
17 individual at risk of identity theft or may compromise the
18 individual's personal safety. Chapter 487N, which requires the
19 public to be notified of data breaches, is not comprehensive
20 enough, as presently written, to cover the additional
21 identifiers. Especially in light of increased digital activity

H.B. NO. 2572
H.D. 2
S.D. 1
Proposed

1 users engage in because of the COVID-19 pandemic, the definition
2 of "personal information" in chapter 487N, Hawaii Revised
3 Statutes, should be updated and expanded to include various
4 ~~personal identifiers and~~ data elements that are found in more
5 comprehensive laws.

6 Additionally, the high transmissibility of the COVID-19
7 virus has lead businesses and governments to consider and
8 implement ways to ~~contact~~ trace the contacts of people that may
9 have been exposed to the virus. Certain proposed methods of
10 contact tracing have included using geolocation data.

11 The task force recommended that explicit consent be
12 required before an individual's geolocation data may be shared
13 or sold to a third party. ~~Numerous reports have arisen in which
14 a person's real time location is identified, allowing the person
15 to be tracked without that person's knowledge or consent by
16 third parties, who in turn share or sell the real time location.
17 This scenario creates serious privacy and safety concerns.~~

18 Residents of Hawaii should be able to share their ~~geolocation~~
19 ~~data~~ contact tracing information with authorized parties to help
20 limit the spread of the novel coronavirus, without sacrificing
21 their privacy or safety.

Commented [KA2]: Contact tracing for COVID is generally not done in real time.

1 Accordingly, the purpose of this Act is to protect Hawaii
2 residents and their personal data in a digital-focused COVID-19
3 society by implementing certain recommendations of the twenty-
4 first century privacy law task force.

5 PART II

6 SECTION 2. Section 487N-1, Hawaii Revised Statutes, is
7 amended as follows:

8 1. By adding two new definitions to be appropriately
9 inserted and to read:

10 ""Identifier" means a ~~common piece of information related~~
11 ~~specifically to an individual, that is commonly used to identify~~
12 ~~that individual across technology platforms, including a first~~
13 ~~name or initial, and last name; a user name for an online~~
14 ~~account; a phone number; or an email address.~~

Commented [KA3]: No other breach law in the country uses this criteria for a data breach law, and inclusion of these largely innocuous data elements would create consumer confusion and needless increased cost for notifications.

15 "Specified data element" means any of the following:

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

Commented [KA4]: A redacted SSN does not present a risk of identity theft, even combined with a name. No other state has this requirement.

18 (2) Driver's license number, federal or state
19 identification card number, or passport number;

20 (3) A federal individual taxpayer identification number;

H.B. NO. 2572
H.D. 2
S.D. 1
Proposed

1 (4) An individual's financial account number or credit or
2 debit card number in combination with any required
3 ~~(5)~~ A security code, access code, personal identification
4 number, or password that would allow access to an
5 individual's financial account;
6 ~~(6)~~ (5) Health insurance policy number, subscriber
7 identification number, or any other unique number used
8 by a health insurer to identify a person;
9 ~~(7)~~ (6) Medical history, ~~m~~Medical treatment by a health
10 care professional, diagnosis of mental or physical
11 condition by a health care professional, or
12 deoxyribonucleic acid profile;
13 ~~(8)~~ (7) Unique biometric data generated from a
14 measurement or analysis of human body characteristics
15 used for authentication purposes, such as a
16 fingerprint, voice print, retina or iris image, ~~or~~
17 ~~other unique physical or digital representation of~~
18 ~~biometric data;~~ and
19 ~~(9)~~ (8) A private key that is unique to an individual and
20 that is used to authenticate or sign an electronic
21 record."

Formatted: Indent: Left: 0.5", Hanging: 0.5", No bullets or numbering

Commented [KA5]: These two paragraphs should be combined, as they are in a number of other state breach notification laws, including AZ (where the electronic signature language below was drawn from) and CA.

1 2. By amending the definition of "personal information" to
2 read:

3 "Personal information" means an ~~[individual's first name~~
4 ~~or first initial and last name in combination with any one or~~
5 ~~more of the following data elements, when either the name or the~~
6 ~~data elements are not encrypted:~~

7 ~~(1) Social security number;~~

8 ~~(2) Driver's license number or Hawaii identification card~~
9 ~~number; or~~

10 ~~(3) Account number, credit or debit card number, access~~
11 ~~code, or password that would permit access to an~~
12 ~~individual's financial account.]~~

13 identifier in combination with one or more specified data
14 elements, when the specified data element or elements are not
15 encrypted or otherwise rendered unreadable. "Personal

16 information" ~~[does]~~ shall not include publicly available
17 information that is lawfully made available to the general
18 public from federal, state, or local government records."

19 SECTION 3. Section 487N-2, Hawaii Revised Statutes, is
20 amended by amending subsection (g) to read as follows:

H.B. NO. 2572
H.D. 2
S.D. 1
Proposed

1 "(g) The following businesses shall be deemed to be in
2 compliance with this section:

3 (1) A financial institution that is subject to the federal
4 Interagency Guidance on Response Programs for
5 Unauthorized Access to Customer Information and
6 Customer Notice published in the Federal Register on
7 March 29, 2005, by the Board of Governors of the
8 Federal Reserve System, the Federal Deposit Insurance
9 Corporation, the Office of the Comptroller of the
10 Currency, and the Office of Thrift Supervision, or
11 subject to 12 C.F.R. Part 748, and any revisions,
12 additions, or substitutions relating to the
13 interagency guidance; and

14 (2) Any health plan or healthcare provider and its
15 business associates that [~~is~~] are subject to and in
16 compliance with the standards for privacy or
17 individually identifiable health information and the
18 security standards for the protection of electronic
19 health information of the Health Insurance Portability
20 and Accountability Act of 1996."

21 PART III

H.B. NO.

2572
H.D. 2
S.D. 1
Proposed

1 SECTION 4. Chapter 481B, Hawaii Revised Statutes, is
2 amended by adding a new section to part I to be appropriately
3 designated and to read as follows:

4 ~~"§481B- Sale of geolocation-contact tracing information~~
5 ~~without consent is prohibited.~~ (a) No person or state
6 agency, in any manner, or by any means, shall sell or offer for
7 sale geolocation-contact tracing information that is recorded or
8 collected through any means by mobile devices or location-based
9 applications without the explicit consent of the individual who
10 is the primary user of the device or application.

11 (b) As used in this section:

12 "Consent" means prior express opt-in authorization that may
13 be revoked by the user at any time a clear affirmative act
14 signifying a freely given, specific, informed, and unambiguous
15 indication of a user's agreement, such as by written statement,
16 including by electronic means, or other clear affirmative
17 action.

18 "Emergency" means the imminent or actual occurrence of an
19 event, which has the likelihood of causing extensive injury,
20 death, or property damage. "Emergency" shall not include the
21 spread of a bacteria or virus.

Commented [KA6]: This definition is a settled definition of "consent" across the business community; in the context of COVID-19 contract tracing, revoking consent is dangerous to public health as it would allow positive cases to prohibit disclosure of such fact.

H.B. NO.

2572
H.D. 2
S.D. 1
Proposed

1 "~~Geolocation~~ Contact tracing information" means information
2 that is:

3 ~~(1) Not the contents of a communication;~~
4 ~~(2)(1) Generated by or derived from, in whole or in~~
5 ~~part, the operation of a mobile device, including but~~
6 ~~not~~
7 ~~limited to a smart phone, tablet, fitness tracker,~~
8 ~~e-reader, or laptop computer; and~~

9 (2) Sufficient to determine or infer the precise location
10 of the identifiable user of the device with precision
11 and accuracy below one thousand seven hundred fifty
12 feet; and

13 (3) Gathered for the purpose of identifying users who were
14 in contact with a person who has tested positive for
15 COVID-19 or was likely exposed to COVID-19.

16 Contact tracing information relates only to information
17 collected following the effective date of this act.

18 ~~(3) Contact tracing information does not include~~
19 ~~information collected by an employer for the purposes of~~
20 ~~ensuring workplace, employee, and customer safety with~~
21 ~~regard to identifying and limiting the spread of COVID-19.~~

Formatted: Indent: Left: 1", No bullets or numbering

Formatted: Indent: Left: 0.5", No bullets or

Formatted: Underline

H.B. NO.

2572
H.D. 2
S.D. 1
Proposed

1 ~~"Location-based application" means a software application~~
2 ~~that is downloaded or installed onto a device or accessed via a~~
3 ~~web browser and collects, uses, or stores geolocation~~
4 ~~information.~~

5 ~~"Precise location" means any data that locates a user~~
6 ~~within a geographic area that is equal to or less than the area~~
7 ~~of a circle with a radius of one mile.~~

8 ~~"Sale" means the exchange of a user's contact tracing~~
9 ~~information for monetary consideration. ~~selling, renting,~~~~
10 ~~releasing, disclosing, disseminating, making available,~~
11 ~~transferring, or otherwise communicating orally, in writing, or~~
12 ~~by electronic or other means, a user's geolocation information~~
13 ~~to another business or a third party for monetary or other~~
14 ~~valuable consideration.~~

15 ~~"Sale" shall not include the releasing, disclosing,~~
16 ~~disseminating, making available, transferring, or otherwise~~
17 ~~communicating orally, in writing, or by electronic or other~~
18 ~~means, a user's ~~geolocation-contact tracing~~ information for the~~
19 ~~purpose of responding to an emergency.~~

H.B. NO. 2572
H.D. 2
S.D. 1
Proposed

1 "Sale" shall not include the transfer of a user's contact
2 tracing information to a service provider who processes the
3 contact tracing data on behalf of the person.

4 "Service Provider" means any legal entity that collects or
5 processes contact tracing data at the direction of a state
6 agency or person.

7 "User" means a person who purchases or leases a device or
8 installs or uses an application on a mobile device and is a
9 resident of Hawaii."

10 PART IV

11 SECTION 5. This Act does not affect rights and duties that
12 matured, penalties that were incurred, and proceedings that were
13 begun before its effective date.

14 SECTION 6. Statutory material to be repealed is bracketed
15 and stricken. New statutory material is underscored.

16 SECTION 7. This Act shall take effect upon its approval.

Commented [KA7]: Necessary in order to avoid dormant commerce clause issues and huge compliance burdens. 91% of positive COVID tests in HI have been from residents, and the state currently requires all visitors to self-quarantine for 14 days upon arrival.

H.B. NO. 2572
H.D. 2
S.D. 1
Proposed

Report Title:

Privacy; Personal Information; Geolocation Information

Description:

Modernizes "personal information" for the purposes of security breach of personal information law. Prohibits the sale of geolocation information without consent. (Proposed SD1)

The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.



June 8, 2020

Senator Rosalyn H. Baker
Chair of the Committee on Commerce, Consumer Protection, and Health
Hawaii Senate
Hawaii State Capitol, Room 230
415 South Beretania Street
Honolulu, HI 96813

Senator Jarrett Keohokalole
Chair of the Committee on Technology
Hawaii Senate
Hawaii State Capitol, Room 203
415 South Beretania Street
Honolulu, HI 96813

RE: Letter in Opposition to HI HB 2572, H.D. 2

Dear Chair Baker and Chair Keohokalole:

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country including many businesses in Hawaii. These companies range from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies, is responsible for more than 85 percent of the U.S. advertising spend and drives more than 80 percent of our nation's digital advertising spend. We and the companies we represent strongly believe consumers deserve meaningful privacy protections supported by reasonable government policies.

While we fully support the legislature's intent to provide Hawaiians with strong privacy protections, we oppose HB 2572 in its current form. The bill includes terms that could significantly limit the availability of data in the marketplace and place economic strain on Hawaii at a time when the state's economy is already in the midst of difficult circumstances.¹ We caution the state legislature against enacting legislation that would detrimentally impact Hawaiians and the economy, particularly during the public health crisis presented by COVID-19 and the severe economic uncertainty facing the world at this time.

HB 2572 contains provisions that could harm consumers' ability to access products and services and exercise choice in the marketplace. The bill also contains particularly onerous terms surrounding digital data that could upend the Internet advertising ecosystem as we know it, disrupting consumers' online experience. While HB 2572 diverges in significant ways from other state privacy laws and privacy bills that are progressing through various state legislatures, it falls short of developing a system that will work well for consumers or enhance a fair and competitive marketplace. In certain respects, the bill attempts to adopt definitions and structural elements of the California Consumer Privacy Act ("CCPA"). However, the CCPA contains various internal inconsistencies and ambiguities, and as such it should not

¹ Hawaii Department of Business, Economic Development & Tourism, *COVID-19 and Hawaii's Economy*, located at <https://dbedt.hawaii.gov/economic/covid19/>.

be used as a basis for legislation in other states. For these reasons, we strongly oppose Hawaii’s HB 2572.²

I. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth

Throughout the past three decades, the U.S. economy has been fueled by the free flow of data. One driving force in this ecosystem has been data-driven advertising. Advertising has helped power the growth of the Internet for years by delivering innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising supports and subsidizes the content and services consumers expect and rely on, including video, news, music, and more. Data-driven advertising allows consumers to access these resources at little or no cost to them, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the Internet’s largest players.

As a result of this advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for the IAB by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.³ Calculating against those figures, the interactive marketing industry contributed \$1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6% of U.S. gross domestic product.⁴

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to valuable content, or the ability to create their own platforms to reach millions of other Internet users. Consumers are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are used to create an enhanced and tailored experience. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. Indeed, as the Federal Trade Commission noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.⁵ It is in this spirit—preserving the ad supported digital and offline media marketplace while helping to design appropriate privacy safeguards—that we provide these comments.

II. The Bill’s Definition of Personal Information for Breach Notification Purposes Extends Beyond Any State Law

HB 2572 would greatly expand the definition of “personal information” subject to the state’s data breach notification law by including identifiers in its scope.⁶ Rendering such identifiers subject to the state’s breach notification statute represents a massive expansion of breach notification requirements far

² HB 2572, 30th Legislature, Reg. Sess. (Haw. 2020) (hereinafter “HB 2572”).

³ John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017), located at <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>.

⁴ *Id.*

⁵ Federal Trade Commission, *In re Developing the Administration’s Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located at https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

⁶ HB 2572, Part II, § 2.

beyond what any other state has done before. Even the CCPA does not include information used to identify individuals across technology platforms in its scope of information subject to the data breach enforcement provisions in the law.⁷ Expanding Hawaii’s definition of “personal information” for data breach notification in this way would make Hawaii be out of step with other states and cause a vastly increased number of notices sent to consumers, thereby unnecessarily raising consumer alarm without providing any additional privacy protections.

The definition of “personal information” for the purposes of Hawaii’s breach notification statute should be comprised of data elements that could enable identity theft if misappropriated. Identifiers across technologies do not pose the same risks to consumers as other data elements that should rightly be included in the scope of breach notification requirements. We therefore recommend that you not alter the definition of personal information for breach notification purposes.

III. The Bill Would Severely Impede Internet Commerce

The bill would also require opt-in consent for any sale of “geolocation information” and “internet browser information,” defined broadly as “information from a person’s use of the internet,” including web browsing history, application usage history, origin and destination IP addresses, device identifiers, and the content of communications comprising Internet activity.⁸ Requiring an opt in to personal information sale is far different from other states’ approaches to personal information in the context of consumer privacy laws. If left uncorrected, HB 2752 would undermine the ad-supported Internet, crippling the online marketplace and resulting in a fractured experience for Hawaiian consumers.

Requiring opt-in consent for the sale of internet browser information and geolocation information as broadly defined would fundamentally change Hawaiians’ ability to access products and services they enjoy and expect through the Internet. This approach diverges from other states’ consumer privacy proposals, such as the CCPA and others that impose an opt out regime to data sales rather than an opt in regime. HB 2572 defines “sale” broadly as “selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means,” geolocation information or internet browser information to another business or a third party for monetary or other valuable consideration.⁹ As a result, any transfer of such data is likely to be treated as a “sale” under the bill, which provides no customary exemptions for service providers or other entities that businesses rely on for various processing activities, and which a consumer would reasonably expect to receive the information. Additionally, consumers would be inundated with requests for their consent to transfer internet browser information, thereby overwhelming them with a variety of notices and requests and causing significant consumer frustration.

Transfers of data over the Internet enable modern digital advertising, which subsidizes and supports the broader economy and helps to expose consumers to products, services, and offerings they want to receive. In a survey commissioned by the Digital Advertising Alliance, 90% of consumers stated that free content was important to the overall value of the Internet and 85% surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers must pay for most content.¹⁰ The survey also found that consumers value the ad-supported content and services at almost \$1,200 a year.¹¹ The opt-in requirements of HB 2572 could

⁷ Cal. Civ. Code § 1798.150(a)(1).

⁸ HB 2572, Part III, § 4.

⁹ *Id.*

¹⁰ Zogby Analytics, Public Opinion Survey on Value of the Ad-Supported Internet (May 2016).

¹¹ Digital Advertising Alliance, Zogby Poll: Americans Say Free, Ad-Supported Online Services Worth \$1,200/Year; 85% Prefer Ad-Supported Internet to Paid, PR Newswire (May 11, 2016).

destroy this model, which consumers have expressed that they value and would not want to see replaced. We therefore respectfully ask you to remove the opt-in consent requirements for “sales” of geolocation information and internet browser information.

* * *

We and our members support Hawaii’s commitment to provide consumers with enhanced privacy protections. However, we believe HB 2572 takes an approach that will severely harm the online economy without providing helpful privacy protections for consumers. We therefore respectfully ask you to reconsider the bill and update it to remove the terms we discussed in this letter so Hawaiians can continue to receive products, services, and offerings they value and expect over the Internet.

Thank you in advance for consideration of this letter.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
202-269-2359

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's
202-355-4564

Christopher Oswald
SVP, Government Relations
Association of National Advertisers
202-269-2359

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau
202-800-0771

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
703-220-5943

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
202-898-0089

Presentation to The
Committee on Commerce, Consumer Protection, and Health
Committee on Technology
June 23, 2020 10:00 a.m.
State Capitol Conference Room 229

Testimony on HB 2572, HD 2, Proposed SD 1 With Comments

TO: The Honorable Rosalyn H. Baker, Chair
The Honorable Jarrett Keohokalole, Chair
The Honorable Stanley Chang, Vice Chair
The Honorable, J. Kalani English, Vice Chair
Members of the Committees

My name is Neal K. Okabayashi, the Executive Director of the Hawaii Bankers Association (HBA). HBA is the trade association representing eight Hawaii banks and two banks from the continent with branches in Hawaii. We wish to make comments on HB 2572, HD 2, proposed SD 1.

We agree with the proposed SD 1, but we do have some concern on the limitation of the use of geolocation data during this pandemic crisis and the likelihood that cases will increase.

One of the thrusts of this bill is to protect privacy when contact tracing is implemented to combat Covid-19. In these pandemic times, there will be a conflict between privacy and public health. At present, there is no evidence that the State of Hawaii is using the data on mobile devices to enforce stay-at-home orders, contact trace, or track those who test positive for Covid-19 but the day may come.

Consideration should be given to provide the State of Hawaii the ability to build apps solely for the purpose of contact tracing but which must be downloaded by the user of a mobile device which downloading shall be deemed to be consent to the use of the app for the transfer of geolocation data but only to the State of Hawaii. The data should be stored on the phone itself, and not the servers of any third party other than the State of Hawaii and the owner of the device. Further, the data received by the state shall not be repurposed for any other purpose. There also should be a sunset date on this exemption of, say, two years since by that time, a viable vaccine should be widely available.

Thank you for the opportunity to submit this testimony to offer our comments on HB 2572, HD 2, proposed SD 1. Please let us know if we can provide further information.

Neal K. Okabayashi
(808) 524-5161

A BILL FOR AN ACT

RELATING TO PRIVACY.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

PART I

SECTION 1. The legislature finds that House Concurrent Resolution No. 225, Senate Draft 1 (2019), established the twenty-first century privacy law task force, whose membership consisted of individuals in government and the private sector with an interest or expertise in privacy law in the digital era. The resolution found that public use of the internet and related technologies has significantly expanded in recent years, and that a lack of meaningful government regulation has resulted in personal privacy being compromised. Accordingly, the legislature requested that the task force examine and make recommendations regarding existing privacy laws and regulations to protect the privacy interests of the people of Hawaii.

The legislature further finds that the task force considered a spectrum of related privacy issues which have been raised in Hawaii and other states in recent years. Numerous states have begun to address the heightened and unique privacy risks that threaten individuals in the digital era of the

twenty-first century. Dozens of states have already adopted components of privacy law contained in this Act. California has enacted a comprehensive privacy act, and states such as Minnesota, New York, Virginia, and Washington are considering comprehensive legislation during their current legislative sessions.

The legislature finds that, following significant inquiry and discussion, the task force made the following various recommendations.

The task force recommended that the definition of "personal information" in chapter 487N, Hawaii Revised Statutes, should be updated and expanded, as the current definition of "personal information" is outdated and needs to be amended. Individuals face too many identifying data elements that, when exposed to the public in a data breach, place an individual at risk of identity theft or may compromise the individual's personal safety. Chapter 487N, which requires the public to be notified of data breaches, is not, in its current form, comprehensive enough to cover the additional identifiers. Accordingly, that chapter's definition of "personal information" should be updated and expanded to include various personal identifiers and data elements that are found in more comprehensive laws.

The task force also recommended that explicit consent be required before an individual's geolocation data may be shared or sold to a third party. Numerous reports have been raised in which a person's real time location is identified, allowing the person to be tracked without that person's knowledge or consent

by third parties, who in turn share or sell the real time location. This scenario creates serious privacy and safety concerns.

The task force also recommended that explicit consent be required before an individual's internet browser history and content accessed may be shared or sold to a third party.

The task force further recommended that, in order to align state law with the holding by the Supreme Court of the United States in *Carpenter v. United States*, 138 S.Ct. 2206 (2018), and current law enforcement practice, the Hawaii Revised Statutes should be amended to:

- (1) Require law enforcement to obtain a search warrant before accessing a person's electronic communications in non-exigent or non-consensual circumstances; and
- (2) Authorize governmental entities to request, and authorize courts to approve, the delay of notification of law enforcement access to electronic communications up to the deadline to provide discovery in criminal cases.

Lastly, the task force recommended that the State protect the privacy of a person's likeness by adopting laws that prohibit the unauthorized use of deep fake technology, which is improving rapidly, and easily sharable on social media.

Accordingly, the purpose of this Act is to implement the recommendations of the twenty-first century privacy law task force.

PART II

SECTION 2. Section 487N-1, Hawaii Revised Statutes, is amended as follows:

1. By adding two new definitions to be appropriately inserted and to read:

"Identifier" means a common piece of information related specifically to an individual, that is commonly used to identify that individual across technology platforms, including a first name or initial, and last name; a user name for an online account; a phone number; or an email address.

"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;
- (7) Medical history, medical treatment by a health care professional, diagnosis of mental or physical condition by a health care professional, or deoxyribonucleic acid profile;

(8) Unique biometric data generated from a measurement or analysis of human body characteristics used for identification authentication purposes, such as a fingerprint, voice print, retina or iris image, or other unique physical or digital representation of biometric data. Unique biometric data does not include a physical or digital photograph unless used or stored for purposes of identifying an individual consumer; and

(9) A private key that is unique to an individual and that is used to authenticate or sign an electronic record."

2. By amending the definition of "personal information" to read:

"Personal information" means an [~~individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:~~

- ~~(1) Social security number;~~
- ~~(2) Driver's license number or Hawaii identification card number; or~~
- ~~(3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.]~~

identifier in combination with one or more specified data elements, when the specified data element or elements are not encrypted. "Personal information" [does] shall not include publicly available information that is lawfully made available

to the general public from federal, state, or local government records."

SECTION 3. Section 487N-2, Hawaii Revised Statutes, is amended by amending subsection (g) to read as follows:

"(g) The following businesses shall be deemed to be in compliance with this section:

- (1) A financial institution that is subject to the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice published in the Federal Register on March 29, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, or subject to 12 C.F.R. Part 748, and any revisions, additions, or substitutions relating to the interagency guidance; and
- (2) Any health plan or healthcare provider and its business associates that [~~is~~] are subject to and in compliance with the standards for privacy or individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996."

PART III

SECTION 4. Chapter 481B, Hawaii Revised Statutes, is amended by adding two new sections to part I to be appropriately designated and to read as follows:

"§481B- Sale of geolocation information without consent is prohibited. (a) No person, in any manner, or by any means, shall sell or offer for sale geolocation information that is recorded or collected through any means by mobile devices or location-based applications without the explicit consent of the individual who is the primary user of the device or application.

(b) As used in this section:

"Consent" means prior express opt-in authorization that may be revoked by the user at any time.

"Emergency" means the imminent or actual occurrence of an event, which has the likelihood of causing extensive injury, death, or property damage.

"Geolocation information" means information that is:

- (1) Not the contents of a communication;
- (2) Generated by or derived from, in whole or in part, the operation of a mobile device, including but not limited to a smart phone, tablet, fitness tracker, e-reader, or laptop computer; and
- (3) Sufficient to determine or infer the precise location of the user of the device.

"Location-based application" means a software application that is downloaded or installed onto a device or accessed via a web browser and collects, uses, or stores geolocation information.

"Precise location" means any data that locates a user within a geographic area that is equal to or less than the area of a circle with a radius of one mile.

"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 (i) for the purpose of responding to an emergency; (ii) at the direction of the consumer; (iii) to a service provider; or (iv) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business.

Formatted: Underline

"User" means a person who purchases or leases a device or installs or uses an application on a mobile device.

§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.

(b) As used in this section:

"Consent" means prior express opt-in authorization which may be revoked by the subscriber at any time.

"Internet browser information" means information from a person's use of the Internet, including:

- (1) Web browsing history;
- (2) Application usage history;
- (3) The origin and destination internet protocol addresses;
- (4) A device identifier, such as a media access control address, international mobile equipment identity, or internet protocol addresses; and
- (5) The content of the communications comprising the internet activity.

"Internet service" means a retail service that provides the capability to transmit data to and receive data through the Internet using a dial-up service, a digital subscriber line, cable modem, fiber optics, wireless radio, satellite, powerline, or other technology used for a similar purpose.

"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. "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 internet browser information (i) at the direction of the

consumer; (ii) to a service provider; or (iii) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business.

"User" means a person who purchases or leases a device or installs or uses an application on a mobile device.

"Subscriber" means an applicant for or a current or former customer of an internet service."

PART IV

SECTION 5. Section 803-41, Hawaii Revised Statutes, is amended by adding a new definition to be appropriately inserted and to read as follows:

"Electronically stored data" means any information that is recorded, stored, or maintained in electronic form by an electronic communication service or a remote computing service. "Electronically stored data" includes the contents of communications, transactional records about communications, and records and information that relate to a subscriber, customer, or user of an electronic communication service or a remote computing service."

SECTION 6. Section 803-47.6, Hawaii Revised Statutes, is amended to read as follows:

"§803-47.6 Requirements for governmental access. (a) ~~[A]~~ Except as otherwise provided by law, a governmental entity may require ~~[the disclosure by]~~ a provider of an electronic communication service ~~[of the contents of an~~

~~electronic communication]~~ and a provider of a remote computing service to disclose electronically stored data pursuant to a search warrant [only.] or written consent from the customer, subscriber, or user of the service.

~~[(b) A governmental entity may require a provider of remote computing services to disclose the contents of any electronic communication pursuant to a search warrant only.~~

~~(c) Subsection (b) of this section is applicable to any electronic communication held or maintained on a remote computing service.~~

~~(1) On behalf of, and received by electronic transmission from (or created by computer processing of communications received by electronic transmission from), a subscriber or customer of the remote computing service; and~~

~~(2) Solely for the purpose of providing storage or computer processing services to the subscriber or customer, if the provider is not authorized to access the contents of those communications for any purpose other than storage or computer processing.~~

~~(d)(1) A provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to, or customer of, the service (other than the contents of any electronic communication) to any person other than a governmental entity.~~

~~(2) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to, or customer of, the service (other than the contents of an electronic communication) to a governmental entity only when:~~

~~(A) Presented with a search warrant;~~

~~(B) Presented with a court order, which seeks the disclosure of transactional records, other than real time transactional records;~~

~~(C) The consent of the subscriber or customer to the disclosure has been obtained; or~~

~~(D) Presented with an administrative subpoena authorized by statute, an attorney general subpoena, or a grand jury or trial subpoena, which seeks the disclosure of information concerning electronic communication, including but not limited to the name, address, local and long distance telephone billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of the service, and the types of services the subscriber or customer utilized.~~

~~(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.~~

~~(e) A court order for disclosure under subsection (d) shall issue only if the governmental entity demonstrates probable cause that the records or other information sought, constitute or relate to the fruits, implements, or existence of a crime or are relevant to a legitimate law enforcement inquiry. An order may be quashed or modified if, upon a motion promptly made, the service provider shows that compliance would be unduly burdensome because of the voluminous nature of the information or records requested, or some other stated reason establishing such a hardship.]~~

(b) Unless otherwise authorized by the court, a governmental entity receiving records or information under this section shall provide notice to the subscriber, customer, or user of the service.

~~[(f)]~~ (c) No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, or subpoena.

~~[(g)]~~ (d) A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a ~~[court order or other process.]~~ search warrant. Records shall be retained for a period of ninety days,

which shall be extended for an additional ninety-day period upon a renewed request by the governmental entity."

SECTION 7. Section 803-47.7, Hawaii Revised Statutes, is amended as follows:

1. By amending subsection (a) to read

"(a) A governmental entity may include in its [~~court order~~] search warrant a requirement that the service provider create a backup copy of the contents of the electronic communication without notifying the subscriber or customer. The service provider shall create the backup copy as soon as practicable, consistent with its regular business practices, and shall confirm to the governmental entity that the backup copy has been made. The backup copy shall be created within two business days after receipt by the service provider of the [~~subpoena or court order~~] warrant."

2. By amending subsection (e) to read:

"(e) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (b) of this section, the subscriber or customer may file a motion to vacate the [~~court order~~] search warrant, with written notice and a copy of the motion being served on both the governmental entity and the service provider. The motion to vacate a [~~court order~~] search warrant shall be filed with the designated judge who issued the [~~order~~] warrant. The motion or application shall contain an affidavit or sworn statement:

(1) Stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications are sought; and

(2) Setting forth the applicant's reasons for believing that the records sought does not constitute probable cause or there has not been substantial compliance with some aspect of the provisions of this part."

3. By amending subsection (g) to read:

"(g) If the court finds that the applicant is not the subscriber or customer whose communications are sought, or that there is reason to believe that the law enforcement inquiry is legitimate and the justification for the communications sought is supported by probable cause, the application or motion shall be denied, and the court shall order the release of the backup copy to the government entity. A court order denying a motion or application shall not be deemed a final order, and no interlocutory appeal may be taken therefrom by the customer. If the court finds that the applicant is a proper subscriber or customer and the justification for the communication sought is not supported by probable cause or that there has not been substantial compliance with the provisions of this part, it shall order vacation of the [~~order~~] warrant previously issued."

SECTION 8. Section 803-47.8, Hawaii Revised Statutes, is amended as follows:

1. By amending subsection (a) to read:

"(a) A governmental entity may as part of a request for a [~~court order~~] search warrant to include a provision that

notification be delayed for a period not exceeding ninety days or, at the discretion of the court, no later than the deadline to provide discovery in a criminal case, if the court determines that notification of the existence of the court order may have an adverse result."

2. By amending subsection (c) to read:

"(c) Extensions of delays in notification may be granted up to ninety days per application to a court~~[,]~~ or, at the discretion of the court, up to the deadline to provide discovery in a criminal case. Each application for an extension must comply with subsection (e) of this section."

3. By amending subsection (e) to read:

"(e) A governmental entity may apply to the designated judge or any other circuit judge or district court judge, if a circuit court judge has not yet been designated by the chief justice of the Hawaii supreme court, or is otherwise unavailable, for an order commanding a provider of an electronic communication service or remote computing service to whom a search warrant, or court order is directed, not to notify any other person of the existence of the search warrant~~[, or court order]~~ for such period as the court deems appropriate not to exceed ninety days~~[,]~~ or, at the discretion of the court, no later than the deadline to provide discovery in a criminal case. The court shall enter the order if it determines that there is reason to believe that notification of the existence of the search warrant~~[, or court order]~~ will result in:

- (1) Endangering the life or physical safety of an individual;
- (2) Flight from prosecution;
- (3) Destruction of or tampering with evidence;
- (4) Intimidation of potential witnesses; or
- (5) Otherwise seriously jeopardizing an investigation or unduly delaying a trial."

PART V

SECTION 9. Section 711-1110.9, Hawaii Revised Statutes, is amended to read as follows:

"§711-1110.9 Violation of privacy in the first

degree. (1) A person commits the offense of violation of privacy in the first degree if, except in the execution of a public duty or as authorized by law:

- (a) The person intentionally or knowingly installs or uses, or both, in any private place, without consent of the person or persons entitled to privacy therein, any device for observing, recording, amplifying, or broadcasting another person in a state of undress or sexual activity in that place; ~~[or]~~
- (b) The person knowingly discloses or threatens to disclose an image or video of another identifiable person either in the nude, as defined in section 712-1210, or engaging in sexual conduct, as defined in section 712-1210, without the consent of the depicted person, with intent to harm substantially the depicted person with respect to that person's health, safety,

business, calling, career, education, financial condition, reputation, or personal relationships or as an act of revenge or retribution; ~~[provided that:]~~ or

(c) The person intentionally creates or discloses, or threatens to disclose, an image or video of a fictitious person depicted in the nude, as defined in section 712-1210, or engaged in sexual conduct, as defined in section 712-1210, that includes the recognizable physical characteristics of a known person so that the image or video appears to depict the known person and not a fictitious person, with intent to harm substantially the depicted person with respect to that person's health, safety, business, calling, career, education, financial condition, reputation, or personal relationships, or as an act or revenge or retribution.

~~[(i)]~~ (2) This ~~[paragraph]~~ section shall not apply to images or videos of the depicted person made:

~~[(A)]~~ (a) When the person was voluntarily nude in public or voluntarily engaging in sexual conduct in public; or

~~[(B)]~~ (b) Pursuant to a voluntary commercial transaction~~+~~ and.

~~[(ii)]~~ (3) Nothing in this ~~[paragraph]~~ section shall be construed to impose liability on a provider of "electronic communication service" or "remote computing service" as those terms are defined in section 803-41, for an image or video

disclosed through the electronic communication service or remote computing service by another person.

~~[(2)]~~ (4) Violation of privacy in the first degree is a class C felony. In addition to any penalties the court may impose, the court may order the destruction of any recording made in violation of this section.

~~[(3)]~~ (5) Any recording or image made or disclosed in violation of this section and not destroyed pursuant to subsection ~~[(2)]~~ (4) shall be sealed and remain confidential."

PART VI

SECTION 10. This Act does not affect rights and duties that matured, penalties that were incurred, and proceedings that were begun before its effective date.

SECTION 11. Statutory material to be repealed is bracketed and stricken. New statutory material is underscored.

SECTION 12. This Act shall take effect on July 1, 2050.

Report Title:

Privacy; Attorney General; Personal Information; Geolocation Information; Search Warrants; Notice; Deep Fakes

Description:

Modernizes "personal information" for the purposes of 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. Prohibits certain manipulated images of individuals. Effective 7/1/2050. (HD2)

June 22, 2020

Senator Rosalyn Baker
Chair, Senate Committee on
Commerce, Consumer Protection and Health
State Capitol, Room 229
Honolulu, HI 96813

Senator Jarrett Keohokalole
Chair, Senate Committee on Technology
State Capitol, Room 229
Honolulu, Hawaii 96813

Re: HB 2572, HD2, Proposed SD1 (Request for Amendment)

On behalf of RELX, a world-leading provider of technology solutions that support the government, insurance, and financial services industries in making communities safer, insurance rates more accurate, commerce more transparent, and processes more efficient, we write to request an amendment that is urgently needed related to the use of geolocation information.

- 1. To protect consumers and help prevent identity theft, an exemption should be included for data that is collected and used to prevent fraud.**

Without a clear fraud exception related to geolocation information, bad actors will have an easier time fraudulently using a consumer's identity. Using geolocation in the application of fraud detection has been proven to increase detection rates and reduce false positives. Geolocation technology can be used to automatically block suspect traffic, request verification (via email or SMS), or flag suspect activity for further internal review. Geolocation can be a key marker to identify suspect proxies, VPNs, other at-risk devices used by would-be identity thieves. In the context of fraud prevention, government agencies partner with private vendors for fraud detection support to identify and respond to greater numbers of suspicious online connections using this digital element.

Requested Amendment

SECTION 4. Chapter 481B

This section shall not apply to any activity involving the collection, maintenance, disclosure, sale, communication, or use of geolocation information to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

Conclusion

We look forward to working with you as this effort continues and offer the expertise of our privacy counsel should you have any questions or require additional materials. Please feel free to contact me at 202-716-7867 or at london.biggs@relx.com if I can be of further assistance.

Sincerely,

London Biggs, Senior Manager, State Government Affairs - West
RELX Inc.



LATE

**TESTIMONY OF TINA YAMAKI
PRESIDENT
RETAIL MERCHANTS OF HAWAII
June 23, 2020**

Re: HB 2572 HD 2 Proposed SD1 RELATING TO PRIVACY

Good morning Chairperson Baker and Chairperson Keohokalole and members of the Senate Committee on Commerce, Consumer Protection and Health and the Committee on Technology. I am Tina Yamaki, President of the Retail Merchants of Hawaii and I appreciate this opportunity to testify.

The Retail Merchants of Hawaii (RMH) is a statewide not-for-profit trade organization committed to supporting the retail industry and business in general in Hawaii. The retail industry is one of the largest employers in the state, employing 25% of the labor force.

The Retail Merchants of Hawaii is opposed to HB 2572 HD2 Proposed SD1 Relating to Privacy. This measure modernizes "personal information" for the purposes of security breach of personal information law. Prohibits the sale of geolocation information without consent.

Retailers main focus is to sell goods and services to our customers. 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.

We feel that this type of legislation is premature as there are a lot of concerns being raised and should be addressed.

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. We do not support exemptions for businesses that have no other equivalent federal or state privacy obligations to protect data, such as the obligations provided by HIPAA and state laws covering protected health information. 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.

Retailers should not be prohibited from offering different prices, rates, levels, or qualities, of goods or services in the context of a customer loyalty program. Loyalty programs are not "financial incentives" and cannot be arbitrarily valuated by state-required mechanisms. Consumers voluntarily participate in loyalty programs and provide personal information so that they may earn benefits and discounts. A recent Forrester research study shows that 72% of adults participate in loyalty programs, and the average adult has signed up for programs with nine different businesses. State laws should not make illegal the types of voluntary programs that

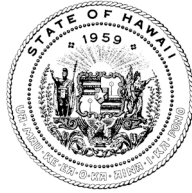
consumers love. Loyalty programs are a major component to many retailers' businesses. Opting into a rewards program at your favorite retailer can provide numerous benefits, including access to private sales, loyalty-based rewards and product discounts, invitations to special events with designers, and much more. Loyalty program participation is a relationship in which consumers receive tangible benefits in exchange for their personal information. These programs are typically offered free of charge and help bolster a relationship between customer and brand. It also ensures that brands can personalize and offer the best products that a consumer wants and needs - and when a customer no longer desires personalized advertisements, they should be empowered to opt out. Customer loyalty program membership increased by 15% between 2015 and 2017. Additionally, 87% percent of customer loyalty program members say they are open to sharing personal information about their activity and behavior in order to receive more personalized rewards. The widespread availability of personal information has increased concerns that this data will be used to discriminate against individuals, but retailers do not charge an individual a higher price for any product or service based on personal information relating to an individual's race, color, religion, national origin, sexual orientation, or gender identity.

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. Taking requests in-store will mean creating additional verification processes which could pose additional security risks. Requiring in-store requests also imposes disproportionate obligations on brick-and-mortar stores, whose data processing is typically of low risk compared to big tech companies and systems (other than those designed to process payment card information) and may not be designed to facilitate processing personal information. Collection of information often takes place closer in time to the benefit provided to the consumer in offline interactions, making the use and purpose obvious.

We ask you to hold this measure

Mahalo for this opportunity to testify.

DAVID Y. IGE
GOVERNOR



DOUGLAS MURDOCK
CHIEF INFORMATION
OFFICER

OFFICE OF ENTERPRISE TECHNOLOGY SERVICES

P.O. BOX 119, HONOLULU, HI 96810-0119
Ph: (808) 586-6000 | Fax: (808) 586-1922
ETS.HAWAII.GOV

Testimony of
DOUGLAS MURDOCK
Chief Information Officer
Enterprise Technology Services

LATE

Before the

SENATE COMMITTEE ON COMMERCE, CONSUMER PROTECTION, AND HEALTH
SENATE COMMITTEE ON TECHNOLOGY
TUESDAY, JUNE 23, 2020

HOUSE BILL NO. 272 HD2, PROPOSED SD1
RELATING TO PRIVACY

Dear Chairs Baker and Keohokalole, Vice Chairs Chang and English, and members of the committee:

The Office of Enterprise Technology Services (ETS) supports HB 2572 HD2, PROPOSED SD1, which redefines "personal information" for the purposes of security breach of personal information law, establishes new provisions on consumer rights to personal information and data brokers, prohibits the sale of geolocation information and internet browser information without consent.

As chair of the Information Privacy and Security Committee created under HRS Section 487N, we support updating the definition of "personal information" in HRS Section 487N that includes expanded identifiers and data elements which are consistent with prevailing practices for current security breach notification laws.

Thank you for the opportunity to provide testimony on this measure.



**Hawaiian
Electric**

**TESTIMONY BEFORE THE SENATE COMMITTEE ON
COMMERCE, CONSUMER PROTECTION, AND HEALTH
&
SENATE COMMITTEE ON TECHNOLOGY**

LATE

H.B. 2572, HD2, PROPOSED SD1

Relating to Privacy

COMMENTS AND REQUESTED AMENDMENTS

Tuesday, June 23, 2020

10:00 a.m.

State Capitol, Conference Room 229

Wendee Hilderbrand
Managing Counsel & Privacy Officer
Hawaiian Electric Company, Inc.

Dear Chair Baker and Chair Keohokalole, Vice Chair Chang and Vice Chair English and Members of the Committees,

My name is Wendee Hilderbrand, and I am testifying on behalf of Hawaiian Electric Company, Inc. (Hawaiian Electric) **with comments on and suggested amendments to H.B. 2572, HD2, PROPOSED SD1**. While Hawaiian Electric is supportive of modernizing Hawaii's data breach statute, several of the provisions in Part II of the proposed legislation go further than the vast majority of other state data security statutes and would lead to significant unintended compliance consequences.

Part II of the bill is intended to update Hawaii's data breach notification statutes, H.R.S. § 487N-1 *et seq.*, by including additional types of data in the definition of "Personal Information," and thereby, expanding the scope of what constitutes a "security breach." Importantly, H.R.S. § 487N-2, like most state data breach notification statutes, has one primary objective: to protect individuals against

identity theft by requiring that they receive notification if certain types of their data (e.g., social security numbers, drivers' license numbers) are compromised, so they can take steps to protect themselves (e.g., credit monitoring, credit freeze).

Part II of H.B. 2572, HD2, PROPOSED SD1 proposes to add health information to the definition of "Personal Information" in H.R.S. § 487N-1. See H.B. 2572, HD2, PROPOSED SD1 Part II, § 2(1)(7). While we agree that health information should be kept confidential and secure, it is not the type of information that subjects individuals to the risk of identity theft, and thus, is ill-suited for H.R.S. § 487N-1. Rather, the confidentiality and security of health information is better addressed by the Health Insurance Portability and Accountability Act ("HIPAA"). HIPAA and its enacting regulations are among the most protective privacy laws in the world; however, they also address considerations unique to health information, such as the business use exception, risk of harm analysis, and implicit consent.

Some of the unintended consequences that could arise if health information is added to H.R.S. § 487N-1 include prohibitions on internal "safety alerts" that advise of workplace injuries as a teaching tool; difficulty in investigating medical leave abuses; impediments to employer-sponsored flu shot or blood drives; prohibitions on workplace wellness challenges or weight loss competitions; and bans on interoffice emails advising of a family illness or birth of a baby. Health information is not related to identity theft, is heavily regulated by HIPAA, and should not be in Hawaii's data breach notification statutes.

Finally, Hawaiian Electric has concerns that Part II of the legislation attempts to expand protection of passwords in a way no other jurisdiction has done, without explanation or reason. Currently, H.R.S. § 487N-1 protects financial account

numbers, as well as passwords that “would permit access to an individual’s financial account.” *Id.* at (3) (emphasis added). H.B. 2572, HD2, PROPOSED SD1 separates account numbers and passwords into two subparagraphs, each with expanded language, but only includes the important qualifying word “financial” in the subparagraph relating to account numbers, inexplicably omitting it from the subparagraph relating to passwords. *Compare id.* at Part II, § 2(1)(4) with § 2(1)(5). This seemingly small omission would result in unprecedented protection of all passwords regardless of what the passcode is connected to (e.g., a Netflix or Snapfish account) or whether it poses any danger of identity theft. No other statute has included such broad protection of passwords, and there is no explanation in the Twenty-First Century Privacy Law Task Force Report as to why the qualifying word “financial” was or should be removed from the subparagraph relating to passwords.

Accordingly, Hawaiian Electric respectfully requests that H.B. 2572, HD2, PROPOSED SD1, Part II, Section 2 be amended by deleting subparagraph (7) regarding health care and adding the word “financial” to subparagraph (5) (i.e., password that would allow access to an individual’s financial account;”). Thank you for your consideration and this opportunity to testify.



1654 South King Street
Honolulu, Hawaii 96826-2097
Telephone: (808) 941.0556
Fax: (808) 945.0019
Web site: www.hcul.org
Email: info@hcul.org



Testimony to the Senate Committees on Consumer Protection, Commerce, and Health;
and Technology
Tuesday, June 23, 2020
State Capitol, Room 229

LATE

Comments on HB 2572, Relating to Privacy, Proposed SD1

To: The Honorable Rosalyn Baker and Jarrett Keohokalole, Chairs
The Honorable Stanley Chang and J. Kalani English, Vice-Chairs
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 in opposition to HB 2572, Relating to Privacy. This bill attempts to modernize the definition of “personal information” for the purposes of security breaches and personal information laws, and prohibits the sale of geolocation information without explicit consent.

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

With regards to the “identifier” definition, we suggest the following: “....means a piece of information that identifies or reasonably could identify, directly or indirectly, an individual including...” This change would remove the “common” wording, which may be applied too broadly, and which could result in unintended consequences.

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.

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



Chamber of Commerce HAWAII

The Voice of Business

Testimony to the Senate Committees on Commerce, Consumer Protection and Health, and Technology

Tuesday, June 23, 2020 at 10:00 A.M.
Conference Room 229, State Capitol

LATE

RE: HB 2572 HD2, PROPOSED SD1, RELATING TO PRIVACY

Chairs Baker and Keohokalole, Vice Chairs Chang and English, and Members of the Committees:

The Chamber of Commerce Hawaii ("The Chamber") **has concerns** with HB 2572 HD2, Proposed SD1, which modernizes "personal information" for the purposes of security breach of personal information law and prohibits the sale of geolocation information without consent.

The Chamber is Hawaii's leading statewide business advocacy organization, representing about 2,000+ businesses. Approximately 80% of our members are small businesses with less than 20 employees. As the "Voice of Business" in Hawaii, the organization works on behalf of members and the entire business community to improve the state's economic climate and to foster positive action on issues of common concern.

The Chamber understands the intent of the bill, including the Proposed SD1 text to address the ongoing COVID-19 pandemic. However, we remain concerned that similar language from previous versions remains in the Proposed SD1. Specifically, the provisions related to "geolocation information" and "internet browser information" rely on a broad definition of "sale" that is now outdated due to amendments made to the California Consumer Privacy Act of 2018. This outdated definition could create unintended consequences for businesses that are trying to comply with the legislation. Additionally, there are also concerns about what the impact on this legislation will have on not just residents of our state, but also on visitors who are trying to access certain services from businesses while here.

The ongoing COVID-19 pandemic has already forced businesses to rethink their entire business model and structure in order to comply with current government and industry guidelines to ensure their employees and customers' safety. As businesses continue to shift towards the new normal of conducting business, including e-commerce, we need to continue to look at ways to help provide them with the tools and assistance to recover and support our economy. The potential of additional costs to businesses to comply with this legislation, added to the financial strain from the ongoing pandemic, could be too much for some of our smaller businesses in the state to be able to recover from.

Thank you for the opportunity to testify in regard to HB 2572 HD2, Proposed SD1.

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

LATE

June 23, 2020

Senator Rosalyn H. Baker, Chair, and Senator Stanley Chang, Vice Chair,
and members of the Senate Committee on Commerce, Consumer Protection, and Health
Senator Jarrett Keohokalole, Chair, and Senator J. Kalani English, Vice Chair,
and members of the Senate Committee on Technology
Hawaii State Capitol
Honolulu, Hawaii 96813

Re: **H.B. 2572, H.D. 2 (Privacy)**
Hearing Date/Time: Tuesday, June 23, 2020, 10:00 a.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) modernizes "personal information" for the purposes of security breach of personal information law, and (2) prohibits the sale of geolocation information without consent.

On page 5, line 3 through page 6, line 7 of House Draft 2 of the Bill (and on page 5, line 15 through page 6, line 19 of the Proposed Senate Draft 1 of the Bill), is the following new definition which would amend Hawaii’s existing law regarding security breach of personal information:

“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;

...

We agree that an individual’s entire social security number (i.e. the entire 9 digits) should be included in paragraph (1) of the “specified data element” definition. This would be similar to the other provisions of the proposed “specified data element” definition, e.g. displaying the entire driver’s license number, the entire federal taxpayer identification number, the entire financial account number, etc.

However, the remainder of paragraph (1) of the “specified data element” definition goes too far: it would include as a “specified data element” the **“last four or more digits”** of the 9 digit social security number. In other words, the social security number would not be a “specified data element” if the number was shortened down to the last 3 digits, i.e. xxx-xx-x**321**.

We are unaware of such a statutory approach to shortening or truncating social security numbers (down to the last **3** digits, i.e. xxx-xx-x**321**) in Hawaii or in other states.

In fact, the standard practice in Hawaii and 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. That's currently the practice for courts, the financial industry, and others.

In Hawaii, there are statutes which only prohibit communicating or making publicly available a person's entire social security number, i.e. all 9 digits are protected from being displayed: xxx-xx-xxxx. See HRS Sec. 487J-2 (social security number protection). See also the definition of "confidential personal information" in HRS Sec. 708-800.

There are also Hawaii statutes which require or allow the public display or disclosure of the last 4 digits (i.e. xxx-xx-4321 is allowed to be displayed). For example, see statutes requiring the last 4 digits of an individual's social security number to be part of a judgment that's to be publicly recorded at the Bureau of Conveyances: HRS Secs. 501-151, 502-33, 504-1, and 636-3.

Additionally, there are Hawaii statutes which require redacting or removing only the first 5 digits of the social security number (so that the last 4 digits are displayed, i.e. xxx-xx-4321) and there are other Hawaii statutes which specifically allow for the disclosure or the use of only the last 4 digits (i.e. xxx-xx-4321). For example, see HRS Secs. 15-4, 232-7, 232-18, 576D-10.5, and 803-6.

However, as stated above, this Bill and the Proposed S.D. 1 would go too far. They would include as a "specified data element" the "**last four or more digits**" of the 9 digit social security number. Under the definition, for the purpose of a security breach of personal information, the social security number would not be a "specified data element" if the number was shortened down to the last 3 digits, i.e. xxx-xx-x**321**.

Such a definition in this Bill and in the Proposed S.D. 1 is contrary to standard practices and current statutes. And there could be unintended consequences if this definition becomes law.

Accordingly, we offer two versions of a proposed amendment to this Bill and the Proposed S.D. 1. 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 xxx-x**5-4321** would be a "specified data element, but displaying xxx-xx-4321 would not be.

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].

...

OR

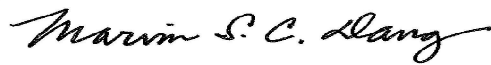
PROPOSED AMENDMENT - VERSION #2:

“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

June 22, 2020

LATE

H.B. 2572 SD1 Proposed - Relating to Privacy

Committee: Senate Committee on Commerce, Consumer Protection, and Health and Committee on Technology

Hearing Date/Time: Tuesday, June 23, 2020, 10:00 AM

Place: Conference Room 229, State Capitol, 415 South Beretania Street

Dear Chairs Baker and Keohokalole, Vice Chairs Chang and English, and members of the Senate Committee on Commerce, Consumer Protection, and Health and Committee on Technology:

I write in **support** of H.B. 2572 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 last year by HCR 225.

In 2006, Hawaii passed a data breach notification law. By 2018, all 50 states had similar laws. Without them, most companies had no obligation to tell consumers when their data was hacked, and we would never have learned of major data breaches like Target and Equifax, affecting 41 million and 147 million consumers respectively.

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

One example of why this update is needed involves medical information, which is especially topical during the COVID-19 crisis. Most of us are familiar with HIPAA, which covers medical information collected and stored by health care providers and insurance companies. But medical information stored by companies like Fitbit, Google or Apple are not subject to HIPAA. It falls to state data breach laws to cover (or not) this information. That's why many states have added medical information to their data breach laws. Hawaii data breach law currently does not cover medical information.

Another example is geolocation information. 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 examples include geolocation data being sold to stalkers and bounty hunters. With the expansion of technology and the topicality of COVID-19 contact tracing, even in the last 3 months, geolocation data is becoming even more valuable commercially. This will exacerbate issues concerning the sale of this very personal information.

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

Kelly McCanlies


Kelly McCanlies

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



Flora Obayashi Testimony for HB2572 HD2

Please pass this bill to protect the privacy of Hawaii students K-12 and college level. I work at a community college providing math tutoring and supplemental instruction helping students to advance to college level algebra classes. The curriculum is provided by Pearson Education and in order to access instructional materials, students are required to surrender their privacy and agree that their personal information is stored in and/or accessed on servers outside the jurisdiction of the United States. There the personal information may be sold and render Hawaii young people vulnerable and at risk for solicitations and unwanted messages. The specific curriculum that prompted my concern is marketed at the K-12 level and is used at community colleges for remedial math. I am concerned that a substantial database of Hawaii students has already been massed somewhere in a foreign country with no privacy protections. Here is a copy of the consent form:



License Agreement and Privacy Policy [Help ?](#)

By registering to use a Pearson Education online learning system, I certify that I have read and agree to the **Pearson License Agreement** and the **Pearson Privacy Policy**.

I understand that my personal information may be stored in and/or accessed from jurisdictions outside of my resident country. I consent to this storage and/or access.

The personal information that I use with a Pearson Education online learning system can include my name and contact information, my answers to questions that are part of the course, my marks on tests or other course requirements, and any comments about me made by my instructor.

[Privacy Policy](#) [?](#)

[Privacy Policy](#)

[License Agreement](#) [?](#)

[License Agreement](#)

Copyright Pearson Education, 1997-2020
[Customer Technical Support](#) | [Privacy Policy](#) | [License Agreement](#)

HB-2572-HD-2

Submitted on: 6/22/2020 1:49:46 PM

Testimony for CPH on 6/23/2020 10:00:00 AM

Submitted By	Organization	Testifier Position	Present at Hearing
Lois Crozer	Individual	Support	No

Comments:

HB-2572-HD-2

Submitted on: 6/19/2020 7:03:51 PM

Testimony for CPH on 6/23/2020 10:00:00 AM

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

Comments:

I am in full support of this bill. Our individual privacy should not be compromised. We should have the option to accept, not an option to refuse.

lynne matusow