



SanHi

GOVERNMENT STRATEGIES

A LIMITED LIABILITY LAW PARTNERSHIP

DATE: February 7, 2023

TO: Senator Jarrett KeohoKalole
Chair, Committee on Commerce and Consumer Protection

FROM: Mihoko E. Ito

RE: **S.B. 1178 Relating to Privacy**
Hearing Date: February 10, 2023 at 9:40 a.m.
Conference Room 229 & Videoconference

Dear Chair Keohokalole, Vice Chair Fukunaga, and Members of Committee:

We submit this testimony on behalf of the Hawaii Bankers Association (HBA). HBA represents seven Hawai'i banks and one bank from the continent with branches in Hawai'i.

HBA submits **comments** regarding S.B. 1178, which amends the definition of "personal information." While we do not object to the substance of the bill, we believe that the bill can be improved by including the amendments we are proposing in this testimony.

We believe that the definition of "Identifier" in its current form is vague as to some elements. Because these identifiers combined with a data element would trigger business obligations if a security breach occurs, we believe the bill should be as specific as possible in defining the identifiers that would trigger a security breach.

1) We would recommend amending the name identifier at page 2, line 19. Using a name by first name or initial as an identifier as the bill currently reads can be problematic, because there are many combinations of names, initials, and last names that people may use when interfacing with businesses. We think more clarity is provided with the following language:

"A name used by an individual, including the combination of the first name, any initials in the name whether at the beginning or middle of the name, or a nickname combined with the last name."

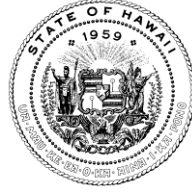
2) We also recommend an amendment to the inclusion of financial account numbers and debit or credit card numbers at page 3, lines 8 and 9. Redacted card numbers are common in data that might be kept in business files, like in credit card receipt records. The risk of harm occurs with these numbers where the entirety of a financial account number or credit/debit card number is released. We would propose to amend this language to read:

“An individual’s financial account number or credit or debit card number unless redacted.”

3) We would also recommend that the exclusion for public information should not be limited to federal, state or local government records. There is no reason that the exception for publicly available information should be restricted to information made available by the government, since that same information could be published by the media, blog, disseminated on television, radio or podcast or otherwise. In some cases, it would be difficult for businesses to ascertain whether information it retained was made available from federal, state, or local government records. We would therefore suggest that this public information exclusion can be improved by deleting “from federal, state, or local government records”, at page 5, lines 2-5 as follows:

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

Thank you for the opportunity to submit this testimony and to offer our proposed amendments. Please let us know if we can provide further information.



STATE OF HAWAII | KA MOKU'ĀINA 'O HAWAI'I
OFFICE OF THE DIRECTOR
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS

NADINE Y. ANDO
DIRECTOR | KA LUNA HO'OKELE

JOSH GREEN, M.D.
GOVERNOR | KE KIA'ĀINA
SYLVIA LUKE
LIEUTENANT GOVERNOR | KA HOPE KIA'ĀINA

DEAN I HAZAMA
DEPUTY DIRECTOR | KA HOPE LUNA HO'OKELE

KA 'OIHANA PILI KĀLEPA
335 MERCHANT STREET, ROOM 310
P.O. BOX 541
HONOLULU, HAWAII 96809
Phone Number: (808) 586-2850
Fax Number: (808) 586-2856
cca.hawaii.gov

Testimony of the Department of Commerce and Consumer Affairs

Before the
Senate Committee on Commerce and Consumer Protection
Friday, February 10, 2023
9:40 AM
Conference Room 229 & Via Videoconference

On the following measure:
S.B. 1178, RELATING TO PRIVACY

Chair Keohokalole and Members of the Committee:

My name is Mana Moriarty, and I am the Executive Director of the Department of Commerce and Consumer Affairs' (Department) Office of Consumer Protection. The Department supports this bill but recommends the following amendments.

The purpose of this bill is to modernize the definition of "personal information" for the purpose of notifying affected persons of data and security breaches.

As currently drafted, the definition for "Identifier" does not protect the privacy of individuals who provide a landline number on records and/or documents that would fall under the definition of "Specific data element." By deleting the word "mobile" in the definition of "Identifier" and simply stating "a phone number" it will protect all individuals who provide a phone number, whether it be a mobile or a landline number, in combination with one or more specific data elements.

Hawaii also has a significant military presence, and servicemembers in the State may use their military identification numbers while doing business in Hawaii. The

Department recommends adding language to include “military identification numbers” under the definition of “specified data element.” This addition will protect the privacy of servicemembers in Hawaii who use their military identification numbers.

Generally, the Department supports S.B. 1178’s expansion of the definition “personal information” in Hawaii Revised Statutes (HRS) chapter 487N, with the Department’s recommended amendments, 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. Hawaii is far from unique in this regard. 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 security breach notification laws were enacted in 2006, and codified at 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 a law requiring notification of security breaches, the definition of personal information has not been updated since the law’s enactment years ago, and advancements in technology have made identity theft far easier than it when the law was enacted. Businesses and government agencies now collect far more information than before, and bad actors exploit vulnerabilities in computer databases for nefarious purposes with increased frequency.

S.B. 1178 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.

Thank you for the opportunity to testify on this bill.

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

February 10, 2023

Senator Jarrett Keohokalole, Chair
Senator Carol Fukunaga, Vice Chair
and members of the Senate Committee on Commerce & Consumer Protection
Hawaii State Capitol
Honolulu, Hawaii 96813

Re: **S.B. 1178 (Privacy)**
Hearing Date/Time: Friday, February 10, 2023, 9:40 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: modernizes the definition of "personal information" for the purposes of notifying affected persons of data and security breaches.

Additionally, we offer below a proposed amendment.

In this Bill, “personal information”, for the purpose of a security breach of personal information, means an “identifier” in combination with one or more “specified data elements.” (See page 5, lines 7 through 18.)

Page 3, lines 2 through 17 of this Bill adds following definition of “specified data element”:

“Specified data element” means any of the following:

- (1) **An individual's social security number, either in its entirety or the last four or more digits;**
- (2) Driver's license number, federal or state identification card number, or passport number;
- (3) A federal individual taxpayer identification number;
- (4) An individual's financial account number, or credit or debit card number;
- (5) A security code, access code, personal identification number, or password that would allow access to an individual's account;

...

(bold and yellow highlight added.)

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

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

But we disagree with the wording in the second phrase of paragraph 1 in the definition of “specified data element” which includes “**the last four or more digits**” of an individual’s social security number. As the second phrase is written, a “specified data element” would be when the last 4 or more digits is displayed, including the following: xxx-xx-**4321**.

However, that second phrase is problematic. That’s because the usual practice in Hawaii (in the statutes, in the court rules, and for the financial industry) and in other states is to allow redacting, shortening, truncating, abbreviating, or limiting the display of an individual’s social security number down to the last 4 digits, i.e. xxx-xx-4321.² Because of the current laws and practice, a display of the last 4 digits should not be a “specified data element” for the purpose of a security breach under this Bill.

We wouldn’t object if paragraph 1 is reworded to include as a “specified data element” **more than** the last 4 digits of a social security number. For example, displaying xxx-x**5**-4321 would be a “specified data element.”

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

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

Below are the two alternate versions:

PROPOSED AMENDMENT - VERSION #1:

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

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

“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

STATE PRIVACY & SECURITY COALITION

February 9, 2023

Chair Jarrett Keohokalole
Vice Chair Carol Fukunaga
Committee on Commerce and Consumer Protection
Hawaii State Senate
415 South Beretania Street
Honolulu, HI 96817

Re: SB1178 – Oppose Unless Amended

Dear Chair Keohokalole, Vice Chair Fukunaga, and Members of the Committee on Commerce and Consumer Protection,

The State Privacy & Security Coalition, a coalition of over 30 companies and five trade associations in the retail, payment card, automotive, healthcare, technology, and telecom sectors (nearly all of whom serve consumers in the state of Hawaii) must respectfully take an oppose unless amended position on Senate Bill SB 1178. We would very much like to work with you to improve the legislation with several amendments that would reduce consumer confusion and align Hawaii's data breach notification requirements to be interoperable with other states.

We appreciate the legislature's work on this statute over the past several years. While we do not object to an update of Hawaii's breach statute, the definitions as currently drafted are overbroad; they would benefit from a narrower focus on those elements that truly present a risk of identity theft or other types of consumer fraud to the affected individuals. Overbroad or vague data elements mean that, in many cases, consumers will receive confusing notices that their identities may be at risk when, in reality, no such risk exists.

Our suggested amendments retain the expanded list of Hawaii data elements (financial accounts, biometric information, health information, etc.) while ensuring that consumers would receive notice for events that could in fact put their identities at risk.

Our amendments are as follows:

1. **Delete the "identifier" definition:**

All other states define personal information using a "(first initial/name + last name) + data elements" formulation. We believe it makes sense for Hawaii to add new data elements reflecting a modern online ecosystem, but these should not depart from the formula used by all other states by creating a new category of "identifiers".

This definition would be the only one of its kind across all 50 states; for data breach notification statutes, the concept of alignment is key. In a data breach scenario, having a statute that is aligned with other states' means that notification to state residents is far more efficient. Businesses will not have to segment out Hawaii residents from other states, as they will likely do if the bill advances in its current form.

STATE PRIVACY & SECURITY COALITION

Much of our concern stems from the “common” nature of the information referenced in the definition, from phone numbers to email addresses, these pieces of information are widely available – even publicly available – and would dramatically increase the scope of what could constitute a breach of security. This would be very confusing to consumers. As an example, if a hacker obtains an individual’s unencrypted driver’s license number, it is likely not an increased indicator of risk for that person to have a phone number as well.

To address the issue of unauthorized account access, we offer a solution in our fourth point, below.

2. **Recognize the value of encrypted or unusable information:** Under current Hawaii law, the value of encrypted data is recognized. This is because when information is accessed in an unauthorized manner, there is likely no risk to a Hawaii resident if the information is encrypted or otherwise protected and the hacker does not also have the encryption key. No other state defines a breach of security to include encrypted or otherwise protected information, and Hawaii should not deviate from this practice for multiple reasons. From the consumer’s viewpoint, requiring breach notifications for encrypted or unusable information would result in misleading notices, leading them to believe that their information was available to hackers or cybercriminals, when this was in fact not the case. Additionally, including a safe harbor for unusable encrypted data will further encourage businesses to use these methods to protect data, ultimately keeping local consumers’ data safer from cybercriminals.

3. **Combine Data Elements (4) and (5):** We agree that the existing formulation in the state statute is confusing, but suggest combining the draft elements of (4) and (5), under the definition for “specified data element,” to further clarify that the risk of harm to an individual comes when a cybercriminal has access to both a financial or credit card account number and the password, not one or the other. The vast majority of states (46 out of 50) take a similar approach to the one we are proposing. In fact, these states generally combine the financial/credit card number with “any” security code or access code permitting access. To ensure that our amendments to the statute are not unintentionally read as unreasonably narrowing the language, we have added the “any” modifier to increase that alignment.

4. **Unauthorized Account Access:** Hawaii would be an outlier from all other states by requiring a formal notification process for a business where there are attempts to access a consumer’s online account. Instead, states have developed an approach to provide rapid notification in the manner in which the consumer interacts with business. Many of us commonly receive these emails encouraging us to change our passwords due to suspicious activity. While our offered amendments are tied to the confines of SB 1178, we would be able to support an additional definition under “Personal Information,” as other states include, to read as follows:

“Personal information means **“either: (i) an individual’s first initial or first name, and last name, in combination with one more specified elements, when the personal information is not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable; or (ii) a username or email address, in combination with a password or security question and answer that would permit access to an online account.”** (Bold indicates our new proposed language).

STATE PRIVACY & SECURITY COALITION

The notification method for the scenario in (ii) would also align with other states' provisions, allowing rapid notice for this type of breach and providing consumers with the tools to immediately protect themselves:

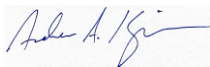
(4) In the case of a security breach involving personal information defined in paragraph (ii) of [the definition of personal information], and no other personal information defined in paragraph (i) of [definition of personal information], the person or business may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change the person's password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same username or email address and password or security question or answer.

In the case of a breach of the security of the system involving personal information defined in paragraph (ii) of [definition of personal information] for login credentials of an email account furnished by the person or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

These provisions allow consumers to be rapidly notified when there is suspicious activity around account credentials, and to be notified in a secure manner; the effect of the second paragraph is to ensure that if, e.g., a consumer's email account has been hacked, the business does not send a password reset link to that email address.

We appreciate your consideration of these issues, and we would be happy to discuss any of the foregoing issues at your convenience.

Respectfully submitted,



Andrew A, Kingman
Counsel, State Privacy & Security Coalition

TO: Members of the Committee on Consumer Protection

FROM: Natalie Iwasa
808-395-3233

HEARING: 9:40 a.m. Friday, February 10, 2023

SUBJECT: SB 1178, Updating Definition of Personal Private Information - **SUPPORT**

Aloha Chairs Keohokalole and Committee Members,

Thank you for allowing the opportunity to provide testimony on SB 1178, which would update the definition of personal private information.

As noted in the preamble, technology has changed the way we live our lives, and it's past time that our laws recognize this. The lists of identifiers and specified data elements appear comprehensive at this point in time.

I therefore support this bill. **Please vote "yes" on SB 1178.**

February 9, 2023

SB 1178 Relating to Privacy
Senate Committee on Commerce and Consumer Protection
Hearing Date/Time: Friday, February 10, 2023, 9:40 AM
Place: Conference Room 229, State Capitol, 415 South Beretania Street

Dear Chair Keohokalole, Vice Chair Fukunaga, and members of the Committee:

I write in **SUPPORT** of SB 1178. As a privacy expert, I have worked in data privacy for over 15 years and served on the 21st Century Privacy Law Task Force created by the Legislature in 2019.

HISTORY:

In 2006, Hawaii passed a data breach notification law (487-N). By 2018, all 50 states had similar laws. Without them, most companies have no obligation to tell consumers when their data is hacked, and we would not learn of major data breaches like Target and Equifax, which affected over 180 million consumers collectively.

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.

CURRENT ISSUES:

One example of why this update is needed is because our state data breach notification law (HRS 487-N) requires a person's name to be compromised, along with sensitive data, in order for a breach to have occurred. To use Chair Keohokalole as an example, the loss of his name (Jarrett Keohokalole) plus his SSN would be a breach, but the loss of his email address (senkeohokalole@capitol.hawaii.gov) and his SSN would not. Since his name and email address are publically available on the state legislature's website, the risk of identity theft is the same in either case, but they are treated completely differently under the current law.

Another example is the question of protecting the last 4 digits of an SSN or the whole SSN. Every person born in Hawaii before 2004 has an SSN that starts with 575 or 576. So the common question "where did you go to high school?" is tantamount to asking what the first 3 digits of their SSN is. For most people here in Hawaii, if the last 4 digits are breached, all that protects their SSN is the middle 2 digits.

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

Kelly McCanlies

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



LATE



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 Committee on Commerce & Consumer Protection
Friday, February 10, 2023
Conference Room 224

Comments re: SB 1178 - Relating to Privacy

To: The Honorable Jarrett Keohokalole, Chair
The Honorable Carol Fukunaga, Vice-Chair
Members of the Committee

My name is Stefanie Sakamoto, and I am testifying on behalf of the Hawaii Credit Union League, the local trade association for 47 Hawaii credit unions, representing over 864,000 credit union members across the state.

HCUL offers the following comments regarding SB 1178, Relating to Privacy. This bill would modernize the definition of “personal information” for the purpose of notifying affected persons of data and security breaches.

While we understand the intent of this bill, we have some concerns. This bill defines “identifier” as a “common piece of information related specifically to an individual, that is commonly used to identify that individual across technology platforms”. We have concerns that “common piece of information” is too broad. The criteria of what constitutes “common” should not be left to interpretation.

Additionally, credit unions and other financial institutions are already required to safeguard sensitive data and financial information via the Gramm-Leach-Bliley Act. We also concur with the testimony presented by the Hawaii Bankers Association.

While we understand the need for data privacy legislation, we would prefer a more comprehensive approach to this issue, to avoid possible unintended consequences for our members.

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



TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Southwest | Telephone 505.402.5738
915 L Street, Suite 1270, Sacramento, CA 95814
www.technet.org | @TechNetSW

February 9, 2023

LATE

Senator Jarrett Keohokalole
Chair, Commerce and Consumer Protection Committee
Hawaii State Capitol
415 South Beretania Street, Room 205
Honolulu, HI 96813

Senator Carol Fukunaga
Vice Chair, Commerce and Consumer Protection Committee
Hawaii State Capitol
415 South Beretania Street, Room 216
Honolulu, HI 96813

Re: SB 1178 (Lee) – Data Breach Notifications– OPPOSE

Dear Chair Keohokalole, Vice Chair Fukunaga and Members of the Committee,

TechNet must respectfully oppose SB 1178 (Lee), a bill that attempts to modernize the state's data breach notification requirements but that may have some unintended consequences.

TechNet is the national, bipartisan network of technology companies that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over five million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

Our member companies place a high priority on consumer privacy. The technology industry is fully committed to securing privacy and security for consumers and engages in a wide range of practices to provide consumers with notice, choices about how their data are used, and control over their data.

We believe this bill is well intentioned, however, the current definitions are overbroad and could lead to confusing notices for consumers in instances when their data isn't at risk. For example, information that is encrypted or otherwise protected presents no risk to consumers if the hacker does not also have the encryption key. Requiring consumers to be notified if this type of information is accessed in a breach would be potentially misleading.

We suggest aligning the definitions and standards in this bill to ensure interoperability with other states. This alignment will ensure consumers receive consistent and efficient notices across state lines, without the need to separate out Hawaiian residents for a distinct notice.

Thank you for your consideration. If you have any questions regarding TechNet's position on this bill, please contact Dylan Hoffman, Executive Director, at dhoffman@technet.org or 505-402-5738.

Sincerely,

A handwritten signature in black ink, appearing to be 'Dylan Hoffman', written over a horizontal line.

Dylan Hoffman
Executive Director for California and the Southwest
TechNet

LATE

SB-1178

Submitted on: 2/9/2023 12:27:29 PM
Testimony for CPN on 2/10/2023 9:40:00 AM

Submitted By	Organization	Testifier Position	Testify
Michael EKM Olderr	Individual	Support	Written Testimony Only

Comments:

I support this bill. Privacy is an ever-changing identity, and we must be constantly vigilant in approaching it and be flexible when defining it.