



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 Judiciary**

**Tuesday, June 30, 2020**

**9:46 a.m.**

**State Capitol, Conference Room 016**

**On the following measure:**

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

**WRITTEN TESTIMONY ONLY**

Chair Rhoads and Members of the Committee:

My name is Stephen Levins, and I am the Executive Director of the Department of Commerce and Consumer Affairs' (Department) Office of Consumer Protection (OCP). The Department appreciates the intent of the bill and offers comments.

The purposes of this bill are to: (1) modernize "personal information" for the purposes of security breach of personal information law; (2) prohibit the sale of contact tracing information without consent; (3) amend provisions relating to electronic eavesdropping law; and (4) prohibit certain manipulated images of individuals.

The Department supports this measure'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of the definition "personal information" in Hawaii Revised Statutes (HRS) chapter 487N because the current definition is obsolete.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.

However, the Department believes the language in H.D. 2 was far more protective of privacy and therefore requests that it be reinserted. H.D. 2 corrected 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 would enhance consumer protections involving privacy and align with legislation recently enacted in other jurisdictions, including Vermont and California

The Department prefers the language in H.D. 2 because it provides broader protection:

“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 authentication purposes, such as a fingerprint, voice print, retina or iris image, or other unique physical or digital representation of biometric data; 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."

As currently written in S.D. 1, the definition of "personal information" is deficient and provides less protection than the definition in H.D. 2. For example, S.D. 1 removes user names for an online account from the list of identifiers and combined passwords with financial account numbers in the list of specified data elements. The effect of this amendment means that the loss of an Amazon user name and password would not be considered a security breach. The Department requests the reinsertion of user names as an identifier and separating passwords from financial account numbers as a specified data element, as was originally drafted in H.D. 2.

Additionally, S.D. 1 amends the "personal information" to include an identifier in combination of a specified data element that is not encrypted or "otherwise rendered unreadable." The Department believes this additional language is too ambiguous and should be deleted.

The Department is concerned with several changes to the list of specified data elements. S.D. 1 removes an individual's last four digits as a specified data element. Individuals who received their social security numbers in Hawaii prior to 2004 are

particularly vulnerable because the social security numbers were issued one of only two prefixes or area numbers: 575 or 576. The middle two numbers, or the group number, were also systematically allocated to the State by the Social Security Administration (SSA) and can be verified on the agency's website. For example, only 31 group numbers were issued for Hawaii residents in 1975. Hawaii residents who applied for a social security number between 2004 and 2011 were issued two area numbers: 750 and 751, and 11 group numbers. To making it more difficult to reconstruct social security numbers using public information, the SSA began randomizing social security numbers in June 2011. As such, the last four digits of a social security number should be included as a specified data element because the first five numbers of social security numbers issued in Hawaii prior to 2011 can easily be reconstructed.

S.D. 1 also removes an individual's medical history as a specified data element. The Department believes that medical history is an important data element because it is information that can be easily linked to an individual. Hacked medical records containing the medical history of an individual can provide enough information to identify, trace, or locate a person, for instance.

S.D. 1 now specifies biometrics used for identification rather than for authentication as a specified data element. Identification is when someone identifies themselves, for example, with a photo on an employee identification card or a user ID on a computer. Authentication is the ability to prove that a user is genuinely whom he or she claims to be. Scanning an employee identification card and a fingerprint at the entrance to the office is an example of authentication because the system verifies the identification by confirming the validity of the identification card and fingerprint scan. As currently written, biometric data used for identification purposes is so broad that it could include driver license photographs, police mugshots, and social media profiles.

With respect to the other elements of S.D. 1, the Department prefers retaining the broader language of H.D. 2's regulation of geolocation data as set forth in part III because it would advance consumer privacy by prohibiting the sale of consumers' location data without their consent. S.D. 1 dramatically changes the focus of the bill to deal with only COVID-19 contact tracing information, rather than the issue of

geolocation. The Department takes no position regarding parts IV and V, since they primarily impact criminal enforcement.

Finally, the Department offers a technical amendment to remove an obsolete reference to the Office of Thrift Supervision. The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 merged the Office of Thrift Supervision into the Office of the Comptroller of the Currency and no longer exists. Accordingly, the reference to “Office of Thrift Supervision” on page 8, line 12 should be deleted.

Thank you for the opportunity to testify on this bill.



To: The Honorable Senator Karl Rhoads, Chair  
The Honorable Senator Jarrett Keohokalole, Vice Chair  
Senate Committee on Judiciary

From: Mark Sektnan, Vice President

Re: **HB 2572 HD2 SD1 Relating to Privacy**  
**APCIA Position: OPPOSE**

Date: Tuesday, June 30, 2020  
9:46 a.m., Room 016

Aloha Chair Rhoads, Vice Chair Keohokalole and Members of the Committee:

The American Property Casualty Insurers Association of America (APCIA) is opposed to HB 2572 HD2 SD1, which amends Hawaii's Security Breach Notification Act and creates restrictions for the sale of geolocation information. Representing nearly 60 percent of the U.S. property casualty insurance market, the American Property Casualty Insurance Association (APCIA) promotes and protects the viability of private competition for the benefit of consumers and insurers. APCIA represents the broadest cross-section of home, auto, and business insurers of any national trade association. APCIA members represent all sizes, structures, and regions, which protect families, communities, and businesses in the U.S. and across the globe.

Consumer privacy and data security are priority issues for the insurance industry and insurers devote considerable resources to protect data, information systems, and consumer trust. To that end, APCIA supports policy efforts that balance corporate responsibility and enhance consumer protection. Unfortunately, HB 2572 HD2 SD1 has potential unintended consequences that may harm rather than protect consumers.

### **Identifier**

The proposed new definition for "identifier" is confusing and implies multiple meanings. For instance, "common usage" could mean "broadly" or "typically" or it could be an individual data element shared across (or common to) different systems. The uncertainty will lead to inconsistent interpretations by businesses. In addition, if interpreted broadly it could unnecessarily lead to over notification of consumers, which will desensitize the consumer to notices when there is a real threat of harm.

We respectfully recommend eliminating the proposed definitions of "Identifier" and "Special Data Elements." Alternatively, the legislature could simply amend the current definition of "Personal Information" to incorporate some of the new data elements proposed in 2572 SD1's definition of "Specified Data Elements." Also, rather than

making an email address and username, an identifier, the legislature could add a data element that reads as follows: “a username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.” This language is consistent with the approach taken in other states.

#### **Specified Data Element – Social Security Number**

The proposed legislation would redefine the social security number (SSN) data element to include a “an individual’s social security number *either in its entirety or the last four or more digits.*” APCIA is aware of no other state that identifies the last four digits of an SSN as an identifier for purposes of the data breach notification trigger. Further, some states include an exemption from the data elements for the last four digits of an SSN. Including the last four digits of a social security number could have the adverse effect of harming security, because it could discourage businesses from implementing security protocols that use only the last four digits of the SSN. As such, we oppose any amendment to the current SSN data element.

#### **Sale of Geolocation Information**

APCIA recommends two edits to the proposed requirements related to the sale of geolocation information. First, there should be an exclusion added to this section that would allow sharing with service providers to perform necessary services. Also, a number of GPS digits, such as 3-4 digits of latitude/longitude, should be included as a minimum for “precise location.” These changes would provide clearer guidance for otherwise vague terms.

For these reasons, APCIA asks that this bill be held in committee.





June 29, 2020

Senator Karl Rhoads, Chair  
Members of the Senate Judiciary Committee  
Hawaii State Capitol, Room 204  
415 South Beretania Street  
Honolulu, HI 96813

**RE: House Bill 2572 SD1**

Dear Chair Rhoads and Members of the Committee:

On behalf of Microsoft, my name is Jonathan Noble and I am the Director, U.S. Government Affairs for Microsoft Corporation and thank you for the opportunity to provide comments to HB 2572 SD1. I am writing to applaud the legislature's efforts to ensure that as government and industry develops and deploys technologies to track, trace, and stem the spread of COVID-19, people's privacy will be protected. Specifically, we support the goals that underly section 4 of HB 2572, relating to contact tracing. While addressing a global problem of the magnitude presented by COVID-19 understandably creates an urgent need for innovative uses of data to fight the pandemic, we believe that any measures deployed must also protect privacy. Indeed, any COVID-19 technological solutions that involve the collection and use of personal data, such as health data, precise geolocation data, proximity or adjacency data, and identifiable contacts, must provide people with certain fundamental safeguards. They must provide people with control of their data and empower people with information that explains how their data will be collected and used. Furthermore, companies need to be accountable and responsible for the data that they collect and use.

However, we are concerned that, as drafted, section 4 of HB 2572 is too narrow and will not provide the public with safeguards necessary to give the public confidence that their privacy will be protected if they use contact tracing applications or similar technologies. For instance, the bill prohibits only the "sale" of contact tracing information, and even then, only does so if the "primary user" does not "consent." It fails to provide individuals with a broader set of rights to more fulsomely control their data. The bill does not require the provision of sufficient information about the collection and use of individuals' data. It defines "contact tracing information" narrowly, such that it may not apply to a broad category of information collected and used by contact tracing apps. Furthermore, the bill fails to create adequate accountability and responsibility requirements for the entities that collect and use data.

We have [set out a series of principles](#) that we believe should apply to the use of tracking, tracing, and testing technologies in response to COVID-19, and encourage you to consider incorporating those



principles in this bill.<sup>1</sup> Specifically, to align with these principles, we would suggest the inclusion of the following requirements for contact tracing apps:

- Obtain meaningful consent, including by being fully transparent about the purpose for data collection, the type of data that will be collected, and the time period the data will be held.
- Any data collected should be used only for contact tracing or public health purposes.
- Limit the collection of data to only that which is necessary for contact tracing purposes.
- Provide appropriate safeguards to secure the data, including de-identification, encryption, or other similar measures to protect information from harmful exposure.
- Delete data as soon as it is no longer needed for the emergency.

Our approach is grounded in the belief that, for technology to succeed, people need to be in control of their data, and be empowered with information that explains how their data will be collected and used. Furthermore, companies need to be accountable and responsible for this data.

We recognize that we do not have all the answers to all of the difficult issues relating to privacy and efforts to combat the COVID-19 pandemic. We look forward to working with you on HB 2572 and would be happy to discuss any questions, comments, or concerns that you may have regarding our feedback. Thank you for the opportunity to provide comments.

---

<sup>1</sup> See "Preserving privacy while addressing COVID-19" on the [Microsoft On the Issues](https://blogs.microsoft.com/on-the-issues/2020/04/20/privacy-covid-19-data-collection/) blog, *available at:* <https://blogs.microsoft.com/on-the-issues/2020/04/20/privacy-covid-19-data-collection/>.

# 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 30, 2020

Sen. Karl Rhoads, Chair, and Sen. Jarrett Keohokalole, Vice Chair  
and members of the Senate Committee on Judiciary  
Hawaii State Capitol  
Honolulu, Hawaii 96813

Re: **H.B. 2572, H.D. 2, S.D. 1 (Privacy)**  
**Hearing Date/Time: Tuesday, June 30, 2020, 9:46 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** on this Bill.

This Bill would: (1) modernize "personal information" for the purposes of security breach of personal information law; (2) prohibit the sale of contact tracing information without consent; (3) amend provisions relating to electronic eavesdropping law; and (4) prohibit certain manipulated images of individuals. It would be effective 9/1/2020 and would sunset on 9/1/2025.

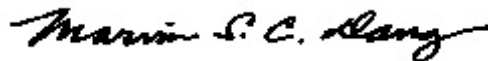
On June 23, 2020, the Senate CPH Committee and Senate TEC Committee jointly held a hearing on the House Draft 2 version and on a proposed Senate Draft 1 version of this Bill. In our written testimony, we expressed a concern about the definition of "specified data" element as it relates to social security numbers for the purpose of a security breach of personal information. We had offered to the Committees an amendment which would replace the problematic definition that was in both the H.D. 2 and the proposed S.D. 1 versions.

Based on the testimonies submitted at the June 23, 2020 CPH/TEC hearing, the Committees revised the problematic definition. The S.D. 1 which was reported from the CPH/TEC Committees on June 26, 2020 does address our concern about the definition of "specified data" element involving social security numbers.

**Accordingly, we support the definition of "specified data" element as it relates to social security numbers for the purpose of a security breach of personal information. See page 6, lines 2 and 3 of S.D. 1.**

We take no position regarding the remainder of the Bill.

Thank you for considering our testimony.



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



**Hawaiian  
Electric**

**TESTIMONY BEFORE THE  
SENATE COMMITTEE ON JUDICIARY**

**LATE**

**H.B. 2572 HD2, SD1**

**Relating to Privacy**

Tuesday, June 30, 2020

9:46 a.m.

State Capitol, Conference Room 016

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

Chair Rhoads, Vice Chair Keohokalole and Members of the Committee,

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, SD1**. While Hawaiian Electric is supportive of modernizing Hawaii's data breach statute, adding medical information to the definition of personally identifiable information ("PII") would go further than the vast majority of other state data security statutes, subject all employers to greater restrictions on the use of medical information than healthcare providers, and lead to a host of 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

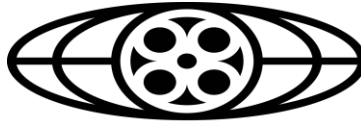
identity theft by requiring that they receive notification if certain types of their data (e.g., social security numbers, drivers' license numbers) are compromised, so they can take steps to protect themselves (e.g., credit monitoring, credit freeze).

Part II of H.B. 2572, HD2, SD1, proposes to add medical information to the definition of "Personal Information" in H.R.S. § 487N-1. See H.B. 2572, HD2, SD1, Part II, § 2(1)(6). While we agree that medical 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 medical 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.

If medical information is added to H.R.S. § 487N-1, which does not contain the same considerations and exceptions as HIPAA, businesses unrelated to healthcare, like Hawaiian Electric, will have to apply even greater protections to medical information than HIPAA places on healthcare entities, like hospitals. Even hospitals are allowed to use healthcare information for business purposes, allowed to disclose healthcare information under circumstances of implied consent, and allowed to determine whether there is a significant risk of harm before notification of disclosure is required. Hawaii's data breach statutes do not include these exceptions and would, therefore, place stricter compliance obligations on employers than HIPAA places on doctors and hospitals.

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; 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.

Accordingly, Hawaiian Electric respectfully requests that H.B. 2572, HD2, SD1, Part II, Section 2 be amended by deleting subparagraph (6) regarding medical information. Thank you for this opportunity to testify.



MOTION PICTURE ASSOCIATION - AMERICA

**LATE**

Written Testimony of the Motion Picture Association – America

In Opposition to Senate Bill 2572, Unless Amended

The Motion Picture Association – America (“MPA-A”), on behalf of its member companies, respectfully opposes Senate Bill 2572, Part V Section 9, unless it is amended. MPA-A’s members<sup>1</sup> are the leading producers and distributors of filmed entertainment content across all platforms, including theatrical motion pictures, broadcast, cable and satellite television, and streaming via the internet.

Part V of S.B. 2572 adds a new subsection (c) to §711-1110.9, which creates a new felony crime for the intentional creation or disclosure of an image of a fictional person that has been altered to make it appear that an actual person is nude or engaging in sexual conduct. This section would make it a felony to create or distribute a “deepfake.” This section of S.B. 2572 is overbroad, inconsistent with the free speech clause of the First Amendment and would likely be struck down by a court.

The U.S. Supreme Court has held that only a few categories of speech fall outside the protections of the First Amendment, including obscenity, child pornography, defamation, speech integral to criminal conduct, fighting words, and speech constituting a grave and imminent threat to public safety. In striking down a federal law criminalizing falsehoods about receiving military honors, the Supreme Court in *United States v. Alvarez*, the Court flatly **rejected** the notion that “false statements receive no First Amendment protection.” 567 U.S. 709, at 719 (2012).

In addition, S.B. 2572 fails to provide appropriate language exempting speech that is protected by the First Amendment, including works of political, public interest, or newsworthy value, and works of parody, satire, commentary, or criticism. *See, e.g., Hustler Magazine, Inc. v. Falwell*, 485 U.S. 46 (1988) (parody protected by First Amendment). Imagine, for example, a video that depicts President Trump as a naked “emperor with no clothes.” The producer of such a video could potentially face a felony prosecution under this bill. MPA-A strongly urges the bill be amended to explicitly exclude these categories of protected speech.

As a practical matter, S.B. 2572 would unduly interfere with the process of making motion pictures, television shows and programs for internet streaming, and potentially subject

---

<sup>1</sup> MPA-A member companies include: The Walt Disney Studios Motion Pictures; Netflix Studios, LLC; Paramount Pictures Corporation; Sony Pictures Entertainment Inc.; Universal City Studios LLC; and Warner Bros. Entertainment Inc.

filmmakers to criminal prosecution. An actor who was dissatisfied with the final version of a movie could assert that the routine editing harmed their business, career, calling, financial condition, reputation or personal relationships. Due to the threat of criminal prosecution, filmmakers would engage in self-censorship and as such this bill could have an unconstitutional chilling effect on speech.<sup>2</sup>

For these reasons, MPA-A respectfully opposes S.B. 2572, unless it is amended.

*June 29, 2020*

---

<sup>2</sup>The Supreme Court has struck down laws due to their chilling effect on speech. *Reno v. ACLU*, 521 U.S. 844 (1997); *Walker v. City of Birmingham*, 388 U.S. 307 (1967)









**HB-2572-SD-1**

Submitted on: 6/28/2020 3:26:39 AM

Testimony for JDC on 6/30/2020 9:46:00 AM

Submitted By	Organization	Testifier Position	Present at Hearing
Dylan Ramos	Individual	Comments	No

## Comments:

Aloha Chair Rhoads, Vice Chair Keohokalole, and Members of the JDC,

Privacy and data rights may be the most important facets of individual liberty in the digital Information Age. The only reason I am not explicitly submitting this under the "support" category for HB2572, HD2, Proposed SD1 is that I believe there is some room for amendment, but only in the interest of consumers and the public, not of corporations intent on exploiting personal data for financial gain.

We need not listen to trade associations' hollow denouncements in the name of business -- we need only look at examples set by the European Union and other places where at least minimal data protections have been successfully adopted. The movement for data rights is progressing; business is and will continue to adapt in clever ways to reach consumers, no government favors required.

That said, certain testimonies submitted for the June 23, 2020 hearing before CPH and TEC do bring up points worthy of review.

1) Testimony by RELX Inc. makes a good point that an exemption for using geolocation data to prevent fraud and identity theft may be beneficial, though I believe strict regulation of this is required and I am skeptical if "sale" is a necessary part of their proposed amendment.

2) Other testimonies, including the one co-signed by six advertising and marketing trade associations, mention the "conflict between privacy and public health" in relation to the fight against COVID-19. I strongly believe that regulating and restricting the use of contact tracing information is a strength of this bill, but I also acknowledge the practicality in their words. I prefer to err on the side of caution in defense of privacy, but I could see room for compromise, perhaps by setting a limited timeframe for such limited data use that ends no later than this year and would require renewal by a supermajority, perhaps even something close to unanimous consent of the State Legislature. This compromise would also involve strictly defining related data use to matters of COVID-19 and provide no opening for applicability to any future public health crises similar to the way U.S. 'forever wars' were enabled by a vague Authorization for Use of Military Force.

3) Please ensure that in the case of this bill's final passage into law, all reconciliations between HD2 and the proposed SD1 to maintain privacy, data protection, and regulations on contact tracing information remain intact.

4) Testimony by Hawaiian Electric includes comments about unnecessary or misplaced amendments regarding the security of health information. I am not enough of a legal expert to parse their complete reasoning, but they do seem to have a point about existing HIPAA protections and regulations. That and their following note about consistency regarding "financial account" information seem worthy of this Committee's review.

There are plenty of moving parts to this bill and quite a few conflicting interests -- many, I'm sure, I did not cover here -- so I am very hopeful that this Committee will make the right decisions.

Mahalo,  
Dylan Ramos  
HD19, SD10 (Kaimuki)

June 29, 2020

HB 2572 SD1 - Relating to Privacy

Committee: Senate Committee on Judiciary

Hearing Date/Time: Tuesday, June 30, 2020, 9:46 AM

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

Dear Chair Rhoads, Vice Chair Keohokalole, and members of the Senate Committee on Judiciary:

I write in **support** of HB 2572 Relating to Privacy, but in **opposition to the amendments** added last week.

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 the 15 years since Hawaii's data breach notification law (HRS 487N) was passed, 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.

However, several amendments were recently added to HB 2572 which alter the intent and jeopardize the ability to implement the provisions therein.

#### Updates to HRS 487N, Definition of Personal Information

- Removing most of the Identifiers:  
By removing most of the Identifiers in the original bill, it requires a person's name for a breach to have occurred under HRS 487-N. That means that my name (K. McCanlies) and my SSN is still a breach, but my email address (kmccanlies@gmail.com) and SSN is not. Similarly, my user ID which is also based on my name, and my SSN is also not a breach. Having these as identifiers makes sense, since these data elements clearly identify a person and can easily be associated to a name.
- Limiting the password to financial accounts.  
By removing user name from the list of Identifiers, and by combining password with the financial account number, this means the loss of an Amazon account user ID and password would not be considered a breach. Same for Target, Walmart, or any online account held outside a financial institution. Additionally, since many people reuse passwords, it is common for hackers to get a user ID and password from a retail breach, then try it at major banks, hoping to gain access to the consumer's financial account. So many large retailers have had breaches, excluding their account user IDs and passwords from the breach notification puts consumer at real risk.
- Last 4 or more digits of SSN  
It is easier to guess the SSN of a person living in Hawaii than for any other US state. People who received their SSNs in Hawaii before 2004 (most adults), only have two possible SSN prefixes – 575 or 576. For the year 1975, when my SSN was issued, only 31 different middle pairs were used. So if you have the last 4 of my SSN, and if my SSN were issued in Hawaii, there are only 62 possibilities. For people who received their SSNs in

Hawaii between 2004 and 2011, it is even easier, as only two prefixes were used (750, 751) and 11 middle pairs, so only 22 possibilities. With the number of combinations so low, it is possible to test the list on any number of websites to determine the actual SSN.

- Identification rather than authentication

One can think about “identification” vs. “authentication” as being analogous to an online account’s user ID and password. The user ID is the identification; it says who you are. The password is authentication; it proves you are who you say.

The bill as amended, now specifies biometrics used for identification. This includes every photo at the DMV, every police mugshot, every set of fingerprints taken by the police, most workplace ID cards, even potentially your profile photo on your Facebook page. This list is huge.

Previously the text applied only to biometrics used for authentication, so biometrics used like a password. If you use a fingerprint to access a building or elevator, or if your face or fingerprint to unlock your phone, the stored electronic file would be included. This list is very small.

In my opinion, this change is so broad, it makes the biometric restriction impossible to implement technically.

#### Geolocation

The modifications to the geolocation text completely invalidate its purpose in the original bill. There is no way to mitigate these modifications. It leaves in place the misalignment that law enforcement needs a warrant to access geolocation data, but the wireless companies can sell to anyone. Add in that currently Hawaii does not use a device or app for contact tracing, in my opinion, renders this part of the bill useless.

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



Kelly McCanlies

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



**LATE**

**HB-2572-SD-1**

Submitted on: 6/30/2020 4:32:13 AM

Testimony for JDC on 6/30/2020 9:46:00 AM

Submitted By	Organization	Testifier Position	Present at Hearing
Flora Obayashi	Individual	Support	No

Comments:

ALOHA,

PLEASE PROTECT THE PRIVACY OF HAWAII'S HIGH SCHOOL AND COLLEGE STUDENTS WHO MUST SURRENDER THEIR PRIVACY RIGHTS IN ORDER TO ACCESS ONLINE EDUCATIONAL CURRICULUM AND INSTRUCTION. PEARSON EDUCATION STORES THIS INFORMATION ON SERVERS OUTSIDE THE JURISDICTION OF THE UNITED STATES WHERE THE INFORMATION MAY BE SOLD OR USED IN HARMFUL WAYS. PLEASE PASS HB2572.

MAHALO



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

**LATE**

**THE HONORABLE KARL RHOADS, CHAIR**  
**SENATE COMMITTEE ON JUDICIARY**  
**Thirtieth State Legislature**  
**Regular Session of 2020**  
**State of Hawai'i**

June 30, 2020

**RE: H.B. 2572, H.D. 2, S.D. 1; RELATING TO PRIVACY.**

Chair Rhoads, Vice Chair Keohokalole, and members of the Senate Committee on Judiciary, the Department of the Prosecuting Attorney, City and County of Honolulu ("Department"), submits the following testimony in support of H.B. 2572, H.D. 2, S.D. 1.

The Department would like to first thank the committee 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 Task Force members included numerous attorneys, including government attorneys, private sectors attorneys, and even the head of the ACLU in Hawaii.** Despite the wide spectrum of legal input, the Department has become aware that there might be a last-minute concern raised by the Motion Picture Association – America. The Department would note that during the numerous Task Force meetings, no members objected to, or expressed concerns with, the proposal relating to Part V of the bill. In addition, no members of the public objected to, or expressed concerns with Part V when it was heard and passed by a joint House committee in February of this year.

The attorneys who drafted and reviewed Part V, including those on the Task Force, agreed that the language of the proposal was sufficiently narrow, and that the inclusion of a criminal intent provision brought the proposal within both the state and federal constitution. **In fact, the intent provision of Part V is already used in a different part of the existing Violation of Privacy statute. (See §711-1110.9(1)(b), H.R.S.).** Courts have unanimously held that such intent language brings the law within the constitution. The Department would also note that the intent language is currently used in Hawaii's extortion statute; that language has repeatedly passed constitutional challenges.

For all of the foregoing reasons, the Department of the Prosecuting Attorney, City and County of Honolulu supports the passage of H.B. 2572, H.D. 2, S.D. 1. Thank you for the opportunity to testify on this matter.



June 30, 2020

**LATE**

Committee on Judiciary  
Sen. Rhodes, Chair  
Sen. Keohokalole, Vice Chair

The Senate  
The Thirtieth Legislature  
Regular Session of 2020

RE: HB 2572, HD2, SD1 - RELATING TO PRIVACY  
DATE: Tuesday, June 30, 2020  
TIME: 9:46am  
PLACE: Conference Room 016  
State Capitol 415 South Beretania Street, Honolulu HI

Aloha Chair Rhodes, Vice Chair Keohokalole and the Members of the Committees,

Thank you for the opportunity to testify in **support** of part **V of HB2572 HD2, SD1** found on page 20 of the measure.

[SAG-AFTRA](#) represents over 1100 actors, recording artists, and media professionals in our state. We are the professional performers working in front of the camera and behind the microphone.

While there may be concern about protecting First Amendment rights, we would like to remind the committee that this union and its members are acutely aware of the need to protect our country's laws guaranteeing the freedom of expression and the press. In fact, when it comes to the First Amendment, our members are at the front lines, risking their health, safety and personal freedom, [see](#) this most recent statement regarding our member journalists and the Black Lives Matter protests. Additionally, content creation - creative expression as protected by First Amendment, is the very backbone of our industry. We absolutely support any proposed amendments that will strengthen and protect First Amendment rights. However, obscenity, harassment and sexual abuse are not rights guaranteed under the First Amendment.

We work in an industry that has seen tremendous advancement in the technology used to create and disseminate content. This evolution in content creation and distribution has not only led to an exponential growth in production and consumption of content, it has equalized the means of creation, broken down the barriers to entry and allowed for professional looking content created by almost anyone with determination and a smart phone.

However, there is a dark side to all this advancement. This dark side can be summed up by a new word that has entered our lexicon: Deepfakes. The same technology used to create younger versions of actors in movies, or insert actors who are no longer able to perform in movies due to death or unavailability, can now be used to create realistic non-consensual pornographic digital

Mericia Palma Elmore, Executive Director  
SAG-AFTRA Hawaii Local  
[mericia.palmaelmore@sagaftra.org](mailto:mericia.palmaelmore@sagaftra.org)  
Ph: 808-596-0388 • Fax: 808-593-2636  
201 Merchant St Suite 2301 Honolulu, HI 96813

SCREEN ACTORS GUILD - AMERICAN FEDERATION OF  
TELEVISION AND RADIO ARTISTS  
SAGAFTRA.org  
Associated Actors & Artistes of America / AFL-CIO

content. New technologies allow content creators to manipulate images to depict individuals as engaging in sexual activity or as performing in the nude without their consent or participation. Specifically, Internet users can use a publicly available artificial intelligence algorithm to transform still images of a person into live action performance by realistically inserting their face onto the body of a porn performer.

A recent Washington Post article, accessed [here](#), describes how “Fake-porn videos are being weaponized to harass and humiliate women: ‘Everybody is a potential target.’” Just as a smart phone has turned all of us into filmmakers with free and easily accessible distribution avenues (TikTok, Facebook, Instagram etc...), the same technology can be used to violate privacy, harass and abuse, turning unwilling people (mostly women) into porn stars.

This proposed legislation amends HRS 711-1110.9 to include nonconsensual, digitally produced sexually explicit material, such as Deepfakes pornography, among the offences that constitute a violation of privacy in the first degree.

This amendment to HRS 711-1110.9 not only fits squarely within Hawaii’s revenge porn laws, it also fulfills the constitutional mandate set forth in Section 6 of the Hawaii Constitution, requiring the legislature to take affirmative steps to implement rules that guarantee that the people’s right to privacy be recognized and shall not be infringed.

To reiterate, we support any proposed amendments that will strengthen and protect First Amendment rights. We welcome the discussion and would be honored to work with this committee and the Privacy Task Force to find language that protects our citizens from the invasion of privacy, harassment and sexual abuse that arises from the creation and dissemination of deepfake pornography, while protecting our First Amendment rights.

Thank you again for your continued support and please don’t hesitate to contact the SAG-AFTRA Hawaii Local office for more information on this issue as it relates to professional performers.

Respectfully,

Mericia Palma Elmore  
Executive Director SAG-AFTRA Hawaii Local