



**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 Ways and Means**  
**Wednesday, February 22, 2023**  
**9:30 AM**  
**Conference Room 211 and Via Videoconference**

**On the following measure:**  
**S.B. 974, S.D. 1, RELATING TO CONSUMER DATA PROTECTION**

Chair Dela Cruz 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 appreciates the intent and offers comments on this bill.

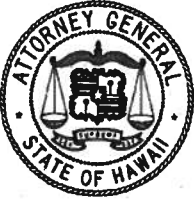
This bill establishes a framework to regulate controllers and processors with access to personal consumer data, establishes penalties for violations, and establishes a new consumer privacy special fund.

This bill creates a comprehensive privacy law that attempts to address important privacy concerns for consumers, such as the nonconsensual sale of personal data by data controllers and processors. This bill creates a consumer bill of rights, including the right to opt out of the sale of personal consumer data, and the right to opt out of the processing of sensitive data. The approach used in this bill borrows from recently enacted legislation in California, Virginia, Connecticut, Colorado, and Utah.

The Executive Director of the Office of Consumer Protection is designated the consumer counsel for the State, and represents and protects the State, the respective counties, and the general public as consumers. The Executive Director investigates reported or suspected violations of laws enacted and rules adopted for the purpose of consumer protection and enforces those laws and rules by bringing civil actions or proceedings. Notwithstanding these duties and functions, this bill places exclusive authority for conducting investigations and bringing enforcement actions with the Department of the Attorney General.

The Office of Consumer Protection requires additional time to study the proposed delegation of exclusive enforcement authority to the Department of the Attorney General. If the Executive Branch is to effectively police data controllers and processors, a robust enforcement framework will be necessary. We would like to ensure that the most appropriate enforcement framework is established from the beginning. Careful study and consultation with the Department of the Attorney General will aid the Office of Consumer Protection in recommending to the Legislature the most effective enforcement mechanism.

Thank you for the opportunity to provide testimony.



**WRITTEN TESTIMONY OF  
THE DEPARTMENT OF THE ATTORNEY GENERAL  
KA 'OIHANA O KA LOIO KUHINA  
THIRTY-SECOND LEGISLATURE, 2023**

---

**LATE**

**ON THE FOLLOWING MEASURE:**

S.B. NO. 974, S.D. 1, RELATING TO CONSUMER DATA PROTECTION.

**BEFORE THE:**

SENATE COMMITTEE ON WAYS AND MEANS

**DATE:** Wednesday, February 22, 2023      **TIME:** 9:30 a.m.

**LOCATION:** State Capitol, Room 211

**TESTIFIER(S):**      **WRITTEN TESTIMONY ONLY. (AMENDED TESTIMONY)**  
(For more information, contact Benjamin M. Creps,  
Deputy Attorney General, at 808-586-1180)

---

Chair Dela Cruz and Members of the Committee:

The Department of the Attorney General (Department) provides the following comments.

The bill creates a new chapter of the Hawaii Revised Statutes, the Consumer Data Protection Act, that establishes a regulatory framework consisting of consumer rights and corresponding corporate responsibilities regarding the collection and use of personal data. The Department notes the following.

First, the proposed law is novel. There is no comprehensive federal law on this subject. Only five states have enacted a regulatory scheme akin to that proposed by this bill, all of which were adopted in 2020. Most of these states' regulatory schemes have or will become effective only this year following an average delayed effective date of two years. Utah's law will be the last to become effective, on December 31, 2023.

Second, the proposed law is highly technical. It covers the specialized subjects of data science, privacy, and security, as well as information systems and networks. The Department is not aware of any state department or agency that has experience in regulating this technical field.

Third, the proposed law is broad in scope. The bill appears to apply to a wide range of businesses, including social-networking companies, gaming companies,

national retailers, search engines, and others that maintain electronic records of customers. These are often national and global corporations with significant resources.

Fourth, it is an open question how to best implement the regulation in Hawaii. Because this is a new field of regulation for the State, it is unclear how the regulation would impact the State and its departments, which department or agency should be vested with regulatory authority, and how the regulation should be enforced. It is also difficult to ascertain what resources would be needed to investigate and prosecute alleged violations.

We note that the resource requirements in other states vary. California created an entirely new agency, with an appropriation of approximately \$10 million. Other states added to their existing consumer protection programs with an appropriation of several hundred thousand dollars. In Hawaii, existing consumer-protection programming is largely administered by the Office of Consumer Protection, Department of Commerce and Consumer Affairs.

Thank you for the opportunity to present this testimony.

**CALIFORNIA PRIVACY PROTECTION AGENCY**

2101 Arena Blvd  
Sacramento, CA 95834  
www.cppa.ca.gov



**Written Testimony of Maureen Mahoney  
Deputy Director of Policy & Legislation, California Privacy Protection Agency**

**Comments on SB 974 (Consumer Data Protection)  
Hawaii Senate Ways and Means Committee**

Chair Dela Cruz, Vice Chair Keith-Agaran, and Members of the Senate Ways and Means Committee, the California Privacy Protection Agency<sup>1</sup> (CPPA or Agency) thanks you for the opportunity to submit written comments on SB 974 (Consumer Data Protection). Our originating statute, the California Consumer Privacy Act (CCPA), directs the Agency to work with other entities with jurisdiction over privacy laws to “ensure consistent application of privacy protections.”<sup>2</sup> We are proud that states are leading the way on legislation to protect consumers’ privacy and data security. As of 2023, four states have adopted, and over half the states have considered, omnibus consumer privacy laws.<sup>3</sup>

The Agency is encouraged that SB 974 shares similarities with California’s approach. For example, SB 974, like the CCPA, not only provides consumers with the right to access, delete, correct, and stop the sale of information to third parties, with additional protections for sensitive data, but is intended to be easy for consumers to use. This reflects the concerns outlined in the California law’s findings, which pointed out the “asymmetry of information [that] makes it difficult for consumers to understand what they are exchanging[.]”<sup>4</sup>

## **Background**

California has a long history of privacy and data protection legislation. In 1972, California voters established the right of privacy in the California Constitution, amending it to include privacy as one of Californians’ “inalienable” rights.<sup>5</sup> In 2002, California became the first state to pass a data breach notification requirement, and in 2003, became the first state to require businesses to post privacy policies outlining their data use practices. In 2018, it became the first state in the nation to adopt a comprehensive commercial privacy law, the California Consumer Privacy Act. That measure went into effect on January 1, 2020, and the Attorney General began enforcing it on July 1, 2020.<sup>6</sup>

In November 2020, California voters ratified Proposition 24, the California Privacy Rights Act, which amends and expands the CCPA, including by creating the first authority with full administrative powers focused on privacy and data protection in the United States, the California Privacy Protection Agency.

---

<sup>1</sup> Established in 2020, the California Privacy Protection Agency was created to protect Californians’ consumer privacy. The CPPA implements and enforces the California Consumer Privacy Act. It is governed by a five-member board that consists of experts in privacy, technology, and consumer rights.

<sup>2</sup> Cal. Civ. Code § 1798.199.40(i).

<sup>3</sup> National Conference of State Legislatures, 2022 Consumer Privacy Legislation (updated June 10, 2022), <https://www.ncsl.org/about-state-legislatures/2022-consumer-privacy-legislation>.

<sup>4</sup> Proposition 24, The California Privacy Rights Act § 2 (2020), <https://vig.cdn.sos.ca.gov/2020/general/pdf/top1-prop24.pdf>.

<sup>5</sup> Cal. Cons. Art. 1 § 1.

<sup>6</sup> Cal. Civ. Code § 1798.100 et seq.

Proposition 24 added new substantive provisions to the CCPA, such as new limitations on businesses' collection, use, retention, and sharing of personal information, a right to correction, and additional protections for sensitive data, which went into effect on January 1, 2023. On April 21, 2022, rulemaking authority under the CCPA formally transferred to the Agency. Along with the Attorney General, the Agency is vested with the authority to undertake enforcement to protect Californians' privacy.

## **Overview of California law**

The CCPA includes specific notice requirements for businesses, grants new privacy rights to consumers, and imposes corresponding obligations on businesses. The rights granted to consumers include the right to know what personal information businesses have collected about consumers and how that information is being used, sold, and shared; the right to delete personal information that businesses have collected from consumers; the right to stop businesses' sale and sharing of personal information; and the right to non-discrimination in service, quality, or price as a result of exercising their privacy rights. As of January 1, 2023, California consumers have the right to correct inaccurate personal information the business maintains about them, and the right to limit a business's use and disclosure of sensitive personal information about them to certain business purposes, among other protections.

The CCPA provides additional protections for children under 16. Businesses are not permitted to sell the personal information of consumers if the business has actual knowledge that the consumer is under 16, unless the consumer, or the consumer's parent or guardian in the case of consumers who are under 13, has affirmatively authorized the sale of the consumer's information.

The CCPA covers information that identifies, relates to, or could reasonably be linked with a particular consumer or household—subject to certain exceptions. The measure applies to for-profit businesses that do business in California, collect consumers' personal information (or have others collect personal information for them), determine why and how the information will be processed, and meet any of the following thresholds: have a gross annual revenue of over \$25 million; buy, sell, or share the personal information of 100,000 or more California consumers or householders; or derive 50% or more of their annual revenue from selling or sharing California residents' personal information.

Businesses have corresponding duties, including with respect to:

- *Data minimization and purpose limitations*
  - Businesses' collection, use, retention, and sharing of personal information must be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected.
  - Businesses must not further process personal information in a manner that is incompatible with those purposes.
- *Dark patterns*
  - In obtaining consent from consumers, businesses are prohibited from using "dark patterns," which are defined to mean a user interface "designed or manipulated with the

substantial effect of subverting or impairing user autonomy, decisionmaking, or choice[.]”<sup>7</sup>

## Overview of CPPA Rulemaking

The California Privacy Protection Agency is currently engaged in a formal rulemaking process to issue regulations to further the intent of the CCPA, as amended.<sup>8</sup> On July 8, 2022, the Agency published its notice of proposed action in the California Regulatory Notice Register, beginning the formal rulemaking process. The proposed regulations primarily do three things: (1) update existing CCPA regulations to harmonize them with CPRA amendments to the CCPA; (2) operationalize new rights and concepts introduced by the CPRA to provide clarity and specificity to implement the law; and (3) reorganize and consolidate requirements set forth in the law to make the regulations easier to follow and understand. They place the consumer in a position where they can knowingly and freely negotiate with a business over the business’s use of the consumer’s personal information.

## SB 974 and State Privacy Laws

As noted above, the Agency appreciates that SB 974 shares a number of similarities with California’s approach. It’s important that consumers have effective tools to protect their privacy, as well as default protections that provide key privacy safeguards even without taking additional steps. For example, like California and other states, SB 974 has several provisions that help ensure this ease of use for consumers:

- **Global opt-out.** California, Colorado, and Connecticut each have a provision in their privacy laws requiring businesses receiving opt-out requests to honor requests submitted by browser privacy signals.<sup>9</sup> The CPPA’s proposed regulations reiterate the requirements for an opt-out preference signal that consumers may use to easily opt-out of the sale or sharing of their personal information with all businesses that they interact with online. With the goal of strengthening consumer privacy, the regulations support innovation in pro-consumer and privacy-aware products and services and help businesses efficiently implement privacy-aware goods and services.

The California Attorney General is currently enforcing the browser privacy signal requirement in the existing CCPA regulations. Last year, it announced its first public case, against Sephora, alleging that Sephora failed to disclose to consumers that it was selling their personal information and failed to process user requests to opt out of sale via user-enabled global privacy controls in violation of the CCPA.<sup>10</sup>

---

<sup>7</sup> Cal. Civ. Code § 1798.140(l).

<sup>8</sup> For more information about the Agency’s work to implement the regulations, please see California Privacy Protection Agency, California Consumer Privacy Act Regulations, [https://cppa.ca.gov/regulations/consumer\\_privacy\\_act.html](https://cppa.ca.gov/regulations/consumer_privacy_act.html).

<sup>9</sup> See, Cal. Civ. Code § 1798.135(e).

<sup>10</sup> Press release, *Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act* (Aug. 24, 2022), <https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement>. For information on additional AG enforcement activity, see State of California Department of Justice, CCPA Enforcement Case Examples (updated Aug. 24, 2022), <https://oag.ca.gov/privacy/ccpa/enforcement>.

- ***Prohibition on dark patterns.*** California, Colorado, and Connecticut all have a provision prohibiting businesses from using dark patterns, defined in California as “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation[,]” in obtaining consent.<sup>11</sup> California’s proposed regulations set forth clear requirements for how businesses are to craft their methods for submitting consumer requests and obtaining consumer consent so that the consumer’s choice is freely made and not manipulated, subverted, or impaired through the use of dark patterns. They address not only narrow situations where consent must affirmatively be given, but general methods for submitting CCPA requests to address abuse by businesses who craft methods in ways that discourage consumers from exercising their rights.<sup>12</sup>
- ***No requirement for verification to opt out.*** Like SB 974, neither the CCPA nor Connecticut’s privacy law require verification of opt-out requests. Verification often creates friction for consumers, making it more difficult for consumers to exercise their rights. This is particularly important as online identifiers that are used for behavioral tracking cannot be easily accessed or verified by the consumer. Like SB 974, California and Connecticut do require identity verification for access, deletion, and correction requests, where consumer privacy could be undermined in the case of an unauthorized request.

However, there are some elements of California law that are not included in SB 974. For example:

- ***Broad definition of personal information.*** California has a broad definition of personal information, including “information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.” It also specifically identifies online identifiers, inferences, and pseudonymous identifiers as personal information.<sup>13</sup>
- ***Protections with respect to non-discrimination/loyalty programs.*** The CCPA prohibits businesses from discriminating against consumers for exercising any of the rights provided by the measure, including by denying goods or services, offering a different price or a different level of quality for goods or services, or retaliating against an employee. Businesses are permitted to charge a consumer a different price or rate, or provide a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer’s data. Businesses are not permitted to use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.<sup>14</sup>

---

<sup>11</sup> Cal. Civ. Code § 1798.140(l)

<sup>12</sup> See, California Privacy Protection Agency, Draft Final Regulations Text at § 7004 (Feb. 3, 2023), [https://coppa.ca.gov/meetings/materials/20230203\\_item4\\_text.pdf](https://coppa.ca.gov/meetings/materials/20230203_item4_text.pdf).

<sup>13</sup> See, Cal. Civ. Code § 1798.140(v).

<sup>14</sup> Cal. Civ. Code § 1798.125.



## **Conclusion**

We hope that our work in implementing the CCPA is helpful to you as you consider legislation. I am happy to answer any questions.



1003 Bishop Street  
Honolulu, Hawaii 96813  
Telephone (808) 525-5877

**Alison H. Ueoka**  
President

## TESTIMONY OF ALISON UEOKA

---

COMMITTEE ON WAYS AND MEANS  
Senator Donovan M. Dela Cruz, Chair  
Senator Gilbert S.C. Keith-Agaran, Vice Chair

Wednesday, February 22, 2023  
9:30 a.m.

### **SB 974, SD1**

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

Hawaii Insurers Council submits comments on this measure. While we support the intent to protect consumers privacy, we ask for **one amendment to the bill.** In 2021, the Hawaii Legislature enacted a National Association of Insurance Commissioner's (NAIC) model law on Data Security. This law is specific to the regulation of entities and the data they collect within and affiliated with the insurance industry. **Therefore, we ask that Section -2(c) be amended to add an exemption to read, "Nonpublic information collected by any licensee, or in any licensee's possession, custody or control, that is subject to the Insurance Data Security Law pursuant to Article 3B, Chapter 431."**

Thank you for the opportunity to testify.

# STATE PRIVACY & SECURITY COALITION

February 21, 2023

Chair Donovan M. Dela Cruz  
Vice Chair Gilbert S.C. Keith-Agaran  
Committee on Ways and Means  
Hawaii State Senate  
415 South Beretania Street  
Honolulu, HI 96817

**Re: SB 974 (Omnibus Privacy) – Request for Amendments**

Dear Chair Dela Cruz, Vice Chair Keith-Agaran, and Members of the Committee on Ways and Means,

The State Privacy & Security Coalition (SPSC), a coalition of over 30 companies and five trade associations in the telecom, retail, technology, automobile, payment card, and health care sectors, writes with suggested amendments to Senate Bill 974. We appreciate that Hawaii is taking a comprehensive approach to privacy legislation and respectfully request consideration of important amendments that more effectively balance increased consumer protections in Hawaii with implementation and compliance by the business community.

This bill is heavily based on the legislation that passed in Connecticut in the spring of 2022. SB 974, like Connecticut's law, provides consumers with a set of strong consumer rights that will provide them increased control over their personal data, as well as increased transparency in how that data is used. It also imposes serious obligations on businesses to collect only the information necessary to accomplish the disclosed purposes for processing, and requires obtaining consent in order to process sensitive data. It requires businesses to document the risks and benefits of processing certain types of data or for particular purposes, and to attempt to mitigate those risks.

We do have some suggestions for how to make this bill clearer, which will also have the effect of aligning it more closely with Connecticut and other states implementing similar laws:

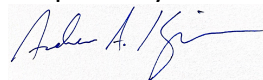
- The bill currently lacks trade secrets protections that make it clear companies do not have to turn over data that would reveal trade secrets; this avoids costly litigation further on in the process;
- The opt-out of profiling is not limited to solely automated profiling as it is in Connecticut. The consequence of this is that consumers may exercise their right to opt-out of processes that have a mix of human review and automated profiling; we believe this is what the intent of the right is and, as in Connecticut, would support this clarification. Consumers likely do not want to be relegated to fully analog processes that are subject to greater degrees of human error than processes that have a mix of human review and automated processing.

# STATE PRIVACY & SECURITY COALITION

- The Gramm-Leach-Bliley exemption language should be modified to exempt “financial institutions or data” subject to the Gramm-Leach-Bliley statute and regulations, as nearly every other state privacy law has done.
- While SB 974 does not include the concept of a global opt-out mechanism, it does retain a confusing sentence in §4, lines 8-12 on page 29. For purposes of clarity, we recommend striking this sentence. Global opt-out mechanisms are still extremely nascent in their development, and the inclusion of this sentence without the corresponding requirements that appear in the Connecticut bill will detract from this bill’s clarity and ability to be implemented.
- There is a typo in §6(b)(5) on page 29 that has carried over from the original language in the Virginia privacy law; the phrase “in accordance with subsection (c)” should be struck.
- There are redundant non-discrimination provisions in §5(a)(5), §5(a)(7), and §5(f) that we would recommend reconciling for clarity’s sake.
- The exception for the pseudonymous data in § 8(e) sets forth a standard that is not aligned with the same provision in the CT or CO laws, and that conflicts with the definition of pseudonymous data in this bill and the other state laws. We would recommend aligning the exception with the CT or CO laws for clarity and interoperability.
- We respectfully request that the rulemaking process be removed. In California, we have seen that rulemaking can often turn into a lengthy process that frustrates compliance efforts.

However, we are happy to continue having discussions on this bill as it moves forward, as it represents a more effective, more sustainable approach for both Hawaii consumers and Hawaii businesses alike.

Respectfully submitted,



Andrew A. Kingman

Counsel, State Privacy & Security Coalition



February 21, 2023

Senator Donovan Dela Cruz  
Hawaii State Capitol, Room 208  
415 South Beretania Street  
Honolulu, HI 96813

Dear Chair Dela Cruz:

BSA | The Software Alliance<sup>1</sup> supports strong privacy protections for consumers and appreciates the Senate Committee on Commerce and Consumer Protection's work to improve consumer privacy through Senate Bill 974 (SB974). In our federal and state advocacy, BSA works to advance legislation that ensures consumers' rights — and the obligations imposed on businesses — function in a world where different types of companies play different roles in handling consumers' personal data. At the state level we have supported strong privacy laws in a range of states, including consumer privacy laws enacted in Colorado, Connecticut, and Virginia.

BSA is the leading advocate for the global software industry. Our members are enterprise software and technology companies that create the business-to-business products and services to help their customers innovate and grow. For example, BSA members provide tools including cloud storage services, customer relationship management software, human resource management programs, identity management services, and collaboration software. Businesses entrust some of their most sensitive information — including personal data — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations, and their business models do not depend on monetizing users' data.

We appreciate the opportunity to share our feedback on SB974. Our recommendations below focus on BSA's core priorities in privacy legislation: clearly distinguishing between controllers and processors and ensuring SB 974's interoperability with other state laws.

---

<sup>1</sup> BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Prokon, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

## **I. Distinguishing Between Controllers and Processors Benefits Consumers.**

We are writing to express our support for SB974's clear recognition of the unique role of data processors. Leading global and state privacy laws reflect the fundamental distinction between processors, which handle personal data on behalf of another company, and controllers, which decide when and why to collect a consumer's personal data. Every state to enact a comprehensive consumer privacy law has incorporated this critical distinction. In Colorado, Connecticut, Utah, and Virginia, state privacy laws assign important — and distinct — obligations to both processors and controllers.<sup>2</sup> In California, the state's privacy law for several years has distinguished between these different roles, which it terms businesses and service providers.<sup>3</sup> This longstanding distinction is also built into privacy and data protection laws worldwide and is foundational to leading international privacy standards and voluntary frameworks that promote cross-border data transfers.<sup>4</sup> BSA applauds you for incorporating this globally recognized distinction into SB974.

Distinguishing between controllers and processors better protects consumer privacy because it allows legislation to craft different obligations for different types of businesses based on their different roles in handling consumers' personal data. Privacy laws should create important obligations for both controllers and processors to protect consumers' personal data — and we appreciate SB974's recognition that those obligations must reflect these different roles. For example, we agree with the bill's approach of ensuring both processors and controllers implement reasonable security measures to protect the security and confidentiality of personal data they handle. We also appreciate the bill's recognition that consumer-facing obligations, including responding to consumer rights requests and seeking a consumer's consent to process personal data, are appropriately placed on controllers, since those obligations can create privacy and security risks if applied to processors handling personal data on behalf of those controllers. Distinguishing between these roles creates clarity for both consumers exercising their rights and for companies implementing their obligations.

---

<sup>2</sup> See, e.g., Colorado's CPA Sec. 6-1-1303(7, 19); Connecticut DPA Sec. 1(8, 21); Utah CPA Sec. 13-61-101(12, 26); Virginia CDPA Sec. 59.1-575.

<sup>3</sup> See, e.g., Cal. Civil Code 1798.140(d, ag).

<sup>4</sup> For example, privacy laws in Hong Kong, Malaysia, and Argentina distinguish between "data users" that control the collection or use of data and companies that only process data on behalf of others. In Mexico, the Philippines, and Switzerland, privacy laws adopt the "controller" and "processor" terminology. Likewise, the APEC Cross Border Privacy Rules, which the US Department of Commerce has strongly supported and promoted, apply only to controllers and are complemented by the APEC Privacy Recognition for Processors, which helps companies that process data demonstrate adherence to privacy obligations and helps controllers identify qualified and accountable processors. In addition, the International Standards Organization in 2019 published its first data protection standard, ISO 27701, which recognizes the distinct roles of controllers and processors in handling personal data. For additional information on the longstanding distinction between controllers and processors — sometimes called businesses and service providers — BSA has published a two-pager available [here](#).

## II. Promoting an Interoperable Approach to Privacy Legislation.

Finally, BSA appreciates your efforts to ensure that SB974 creates privacy protections that are interoperable with protections created in other state privacy laws. Privacy laws around the world need to be consistent enough that they are interoperable, so that consumers understand how their rights change across jurisdictions and businesses can readily map obligations imposed by a new law against their existing obligations under other laws.

As an initial matter, we appreciate the harmonized approach you have taken in aligning many of SB974's provisions with the Connecticut Data Privacy Act (CTDPA) and Colorado Privacy Act (CPA). BSA supported the Connecticut, Colorado, and Virginia privacy laws, which build on this same structural model of privacy legislation. In particular, we support SB974's focus on protecting the privacy of consumers, and excluding employment data from the bill's scope and in its definition of "consumer." We also support SB974's approach to enforcement, which provides the Attorney General with exclusive authority to enforce the bill, which we believe will help promote a consistent and clear approach to enforcement. We commend you for drafting SB974's provisions in a manner that is interoperable with protections included in other state privacy laws, which helps drive strong business compliance practices that can better protect consumer privacy.

Thank you for your thoughtful approach in establishing strong consumer privacy protections, and for your consideration of our perspective. BSA would be happy to provide further perspective on this legislation as it progresses through the legislative process.

Sincerely,



Olga Medina  
Director, Policy

CC: Senator Chris Lee



**TECHNET**  
THE VOICE OF THE  
INNOVATION ECONOMY

TechNet Southwest | Telephone 505.402.5738  
915 L Street, Suite 1270, Sacramento, CA 95814  
[www.technet.org](http://www.technet.org) | @TechNetSW

February 21, 2023

Senator Donovan M. Dela Cruz  
Chair, Committee on Ways and Means  
Hawaii State Capitol  
415 South Beretania Street, Room 208  
Honolulu, HI 96813

Senator Gilbert S.C. Keith-Agaran  
Vice Chair, Committee on Ways and Means  
Hawaii State Capitol  
415 South Beretania Street, Room 221  
Honolulu, HI 96813

**Re: SB 974 (Lee) –Data Privacy– Comments**

Dear Chair Dela Cruz, Vice Chair Keith-Agaran and Members of the Committee,

We appreciate the opportunity to provide comments on SB 974 (Lee), a bill that would enact strong privacy protections for Hawaiian consumers.

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. TechNet supports a federal standard that establishes a uniform set of rights and responsibilities for all Americans. Even the most well-designed state statute will ultimately contribute to a patchwork of different standards across the country. Understanding that states will move forward in the absence of federal law, we ask that the Committee consider a few changes to this bill should it move forward.

First, SB 974 should include trade secret protections to make it clear that companies would not have to turn over sensitive information or compromise their intellectual property. This would help avoid costly litigation to protect that information, which in turn will ease the cost of compliance.



Additionally, aligning the standards for pseudonymous data with other state laws like Connecticut and Colorado would help avoid conflicts and ensure interoperability. We also believe some modifications should be made to the global opt-out provisions, the non-discriminatory provisions, and a slight modification to the Gramm-Leach-Bliley exemption would provide much needed clarity.

Finally, we also request the rulemaking process be removed because it is redundant. Notably in California the rulemaking process has become so protracted that final regulations are nearly a year late, which leaves consumers with limited ability to access their rights because companies are adapting to shifting requirements.

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](mailto:dhoffman@technet.org) or 505-402-5738.

Sincerely,

A handwritten signature in black ink, appearing to be 'Dylan Hoffman', written in a cursive style.

Dylan Hoffman  
Executive Director for California and the Southwest  
TechNet



February 21, 2023

Hon. Donovan M. Dela Cruz  
Committee on Ways and Means  
Hawaii State Senate

RE: Senate Bill 974 SD 1 - Consumer Data Protection

Dear Chair Dela Cruz and Members of the Committee:

I am writing to address concerns with Senate Bill 974 SD 1 regarding consumer data protection. As written, the bill would pose serious hardships on the ability of our organization, the National Insurance Crime Bureau (“NICB”) to combat insurance fraud.

### **Organization and Business Purpose**

Headquartered in Des Plaines, Illinois, and with a 110-year history, the NICB is the nation’s premier not-for-profit organization exclusively dedicated to leading a united effort to prevent insurance crime and fraud through intelligence-driven operations. NICB is primarily funded by assessments on our nearly 1,200-member property-casualty insurance companies, car rental companies, and other strategic partners.

NICB sits at the intersection between the insurance industry and law enforcement, helping to identify, prevent, and deter fraudulent insurance claims. NICB’s approximately 400 employees work with law enforcement entities, government agencies, prosecutors, and international crime-fighting organizations in pursuit of its mission. While NICB provides value to our member companies, we also serve a significant public benefit by helping to stem the estimated billions of dollars in economic harm that insurance crime causes to individual policy holders across the country every year.

NICB maintains operations in every state around the country, including in Hawaii where NICB is an unmatched and trusted partner in the fight against insurance fraud. NICB analysts and agents work daily with state and local Hawaii law enforcement and regulatory agencies to provide assistance in all manner of cases. NICB maintains close agency relationships that can directly speak to NICB’s value, including: the Department of Commerce and Consumer Affairs, Honolulu Police Department, Hawaii Police Department, Kaua’i Police Department, Maui Police Department, Hawaii Department of Transportation, the four county departments of motor vehicles, the four county prosecuting agencies, federal law enforcement agencies located in Hawaii, including the Federal Bureau of Investigations, and more.

### **Hawaii’s Insurance Fraud Reporting Requirements**

Recognizing the adverse impact of insurance crime on the citizens of Hawaii, the legislature enacted laws requiring Hawaii insurers to report suspected fraudulent claims to the Hawaii Department of Commerce and Consumer Affairs’ Insurance Fraud Investigations Branch.<sup>1</sup> In the vast majority of cases, insurers submit suspected fraud referrals to NICB through NICB’s Fraud Bureau Reporting Program to meet their reporting

---

<sup>1</sup> HRS § 431:2-409

requirements. In partnership with the National Association of Insurance Commissioners, NICB relays that information to the Insurance Fraud Investigations Branch. The same statute also authorizes the Insurance Fraud Investigations Branch to share information otherwise protected from public disclosure specifically with NICB. Recognizing NICB as a critical information sharing hub, the Hawai'i State Legislature has provided NICB protection from civil liability as well as those who share fraud information with NICB.<sup>2</sup>

### **Applicability of Senate Bill 974 SD 1**

Senate Bill 974 SD 1 exempts nonprofit organizations incorporated under Hawaii chapter 414D as well as those organized under sections 501(c)(3), (6), or (12) of the Internal Revenue Code of 1986. NICB is incorporated as a 501(c)(4) nonprofit organization in the state of Illinois. In Hawaii, NICB is registered as a foreign nonprofit corporation by way of chapter 414D.

### **Proposed Changes and Policy Rationale**

Consistent with longstanding public policy determinations already considered and enacted in Hawaii law, NICB respectfully requests an amendment to ensure its wholesale exemption from the Act. As a 501(c)(4) non-profit entity, NICB is exempt from California, Connecticut, and Utah's comprehensive consumer data privacy laws. Virginia's Consumer Data Protection Act specifically exempts NICB as an entity, as did leading bills introduced in the 2022 and 2023 legislative sessions in Ohio, Washington state, Kentucky, Texas, and Iowa.

The policy reasons for excluding NICB from these burdens are several-fold. First, NICB provides significant benefits to the millions of consumers who are victims of insurance fraud. Second, as a non-profit organization that serves a public interest, NICB is not equally situated with private entities that typically establish more complex compliance infrastructure for private-sector-related obligations. Furthermore, NICB's required responses to individual consumer requests would likely expose otherwise covert criminal investigations. In addition, imposing what is essentially a "compliance, response, reporting and litigation" obligation – without any benefit to consumers – is wholly inconsistent with Hawaii's insurance fraud reporting requirements and civil immunity provisions referenced above. Finally, NICB would not be afforded protection for our operations relating to our natural disaster response. The Geospatial Insurance Consortium (GIC), which is an initiative developed by NICB, has become an integral part of public agencies' overall response plans to significant catastrophic events by providing aerial imagery and other information, at no cost to the public, to help response agencies efficiently allocate their resources to the most heavily impacted areas.

### **Conclusion**

We appreciate your consideration of our concerns. We welcome the opportunity to follow up directly with your staff to discuss these issues in more detail. In the meantime, if you have any questions or need additional information, please contact me at [hhandler@nicb.org](mailto:hhandler@nicb.org) or 312-771-3974.

Sincerely,



Howard Handler, MPPA

Senior Director

Strategy, Policy, and Government Affairs

1111 E. Touhy Ave., Suite 400, Des Plaines Illinois 60018  
800.544.7000 | [www.NICB.org](http://www.NICB.org)

---

<sup>2</sup> HRS § 431:2-409

February 21, 2023

SB 974 SD1 Relating to Privacy  
Senate Committee on Ways and Means  
Hearing Date/Time: Friday, February 22, 2023, 9:30 AM  
Place: Conference Room 211, State Capitol, 415 South Beretania Street

Dear Chair Dela Cruz, Vice Chair Keith-Agaran, and members of the Committee:

I write in **SUPPORT** of SB 974, but with **ONE CONCERN** about version SD1. 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.

How can people not have rights to their own data? SB 974 is a **bill of rights** for consumer data. But in version SD1, one of these rights has been limited to the point of being rendered *meaningless*: the RIGHT TO DELETE. In SD1, the bill was amended so that a consumer only has the right to delete data they originally provided, not data that has been bought, collected, or inferred about them.

**SB974 as amended:** “To delete personal data provided by ~~, or inferred or obtained about,~~ the consumer;”

Please review what other states have done:

**Colorado:** “a consumer has the right to delete personal data concerning the consumer.”

**Connecticut:** “A consumer shall have the right to ... delete personal data provided by, or obtained about, the consumer;”

**Virginia:** “To delete personal data provided by or obtained about the consumer;”

As you can see, other states have enacted a broader RIGHT TO DELETE. Please follow the lead of states like Colorado, Connecticut and Virginia and protect the rights of residents of the state of Hawaii.

Thank you for your consideration and the opportunity testify on this legislation.

*Kelly McCanlies*

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





**Hawaiian  
Electric**

**TESTIMONY BEFORE THE SENATE COMMITTEE ON  
WAYS AND MEANS**

**SB 974 SD1**

**Relating to Consumer Data Protection**

February 22, 2023  
9:30 a.m., Agenda Item #21  
State Capitol, Conference Room 211 & Videoconference

Wendee Hilderbrand  
Managing Counsel & Privacy Officer  
Hawaiian Electric

My name is Wendee Hilderbrand, and I am testifying on behalf of Hawaiian Electric in opposition to SB 974 SD1, as currently drafted, and offer one amendment. Hawaiian Electric strongly supports consumer privacy rights and has already voluntarily implemented many of the requirements of SB 974 SD1. We are also prepared to implement the proposed consumer rights to confirm, to correct, to delete, and to opt out (§ 3(1)-(5)). Hawaiian Electric's only remaining concern is with the right to access (§ 3(1)), which would result in significant compliance costs and unintended consequences.

Hawaiian Electric thanks the Senate Committee on Commerce and Consumer Protection for acknowledging our concerns with the original language of the bill by adopting our proposed amendment to the language of § 3(4), which addresses the consumer right to receive copies. In order to avoid the extensive problems that may occur if businesses are required to turn over confidential internal files, the State of Virginia limited the consumer right to receive copies to "personal data that the consumer previously provided to the controller." The State of Utah adopted the same approach.

However, one ambiguity remains, in § 3(1), which provides consumers the right

“to access the personal data.” Since most data is electronic and exists only in proprietary systems, the only practical way to provide consumers with access to their personal data would be to provide them with copies. Thus, by leaving the language “and to access the personal data” in § 3(1), the bill still provides a general right to copies, thereby defeating the change made to § 3(5).

Notably, this same ambiguity – the right to access – appeared in an early version of companion legislation introduced in the House, HB 1497. Hawaiian Electric raised these same concerns in testimony before the House Committee on Higher Education and Technology. These arguments were also well taken, and the language “and to access the personal data” was deleted from § 3(1) in HB 1497 HD1.

Hawaiian Electric is appreciative of the above-referenced Committees’ efforts to make these changes to the pending legislation, in order to address our concerns while still maintaining the crux of the legislation and the rights it provides Hawaii’s consumers.

We ask for this one final change to SB 974 SD1 – specifically, the deletion of “and to access the personal data” from § 3(1) – to prevent businesses such as ours from having to turn over large quantities of confidential internal files upon request.

On page 15, lines 9-11:

(1) To confirm whether or not a controller is processing the consumer's personal data ~~and to access the personal data;~~

Thank you for the opportunity to provide testimony.



Testimony to the Senate Committee on Ways & Means  
Wednesday, February 22, 2023  
Conference Room 224

Comments re: SB 974 - Relating to Privacy

To: The Honorable Donovan Dela Cruz, Chair  
The Honorable Gil Keith Agaran, 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 974, Relating to Consumer Data Protection.

We understand the need for data privacy and protection legislation, but believe that the best approach moving forward would be to convene a working group in order to delve into the finer details of this proposed legislation. A more comprehensive discussion on data privacy, consumer data protection, and other related issues would be integral to avoid possible unintended consequences for our community.

Further, there are concerns that legislation such as this one may be extremely difficult to both comply with, and enforce. Financial documents go back many years, and the proposed legislation is unclear as to whether or not it will be retroactive to every document in existence. Depending on what "personal data" would be covered by this law, many businesses would find themselves in violation, with any past documents that they have stored. This is one example of the unintended consequences of this legislation, which should be discussed by businesses that would be required to comply.

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



**SanHi**

GOVERNMENT STRATEGIES

A LIMITED LIABILITY LAW PARTNERSHIP

DATE: February 21, 2023

TO: Senator Donovan M. Dela Cruz  
Chair, Committee on Ways and Means  
*Submitted Via Capitol Website*

FROM: Matt Tsujimura

RE: **S.B. 974, SD1 – Relating to Consumer Data Protection**  
**Hearing Date: Wednesday, February 22, 2023 at 9:30AM**  
**Conference Room: 211**

---

Dear Chair Dela Cruz, Vice Chair Keith-Agaran, and Members of the Committee on Ways and Means:

I am Matt Tsujimura, representing State Farm Mutual Automobile Insurance Company (State Farm). State Farm offers this testimony in opposition to S.B. 974 which establishes a framework to regulate controllers and processors with access to personal consumer data.

State Farm understands and shares the Legislature's concern for protecting privacy of information that consumers give to businesses to provide the products and services that consumers desire. The financial services industry, which includes insurers, is highly regulated. Insurer's use of information is regulated through a framework of privacy laws at the state and federal level, including the Gramm-Leach-Bliley Act (GLBA), HIPAA, and HRS §§ 431:2-209, 431:3A-101 to 431:3A-504, and 431:3B-101 to 431:3B-306.

The GLBA, for example, imposes strict privacy provisions to protect customers of financial services entities. The GLBA provides consumers with the right to opt out of sharing nonpublic personal information (NPI) with nonaffiliated third parties and requires financial institutions to provide customers with a privacy policy disclosing: 1) whether the financial institution discloses NPI to affiliates and nonaffiliated third parties, including the categories of information disclosed; 2) whether the financial institution discloses NPI of former customers; 3) the categories of NPI collected by the financial institution; 4) the policies maintained by the financial institution to protect the confidentiality and security of NPI; and 5) disclosure of and ability to opt out of sharing NPI with affiliates.

Under the GLBA, insurers cannot disclose NPI to nonaffiliated third parties without notice and an opportunity to opt out. Exceptions to this general rule—such as the often used “service provider” exception— account for the need to process transactions or to report consumer information to consumer reporting agencies. Under the GLBA, state insurance regulators are the functional regulators for privacy and security of customer personal information held by insurers.



State Farm is concerned S.B. 974 will inadvertently limit its ability to effectively serve its policyholders in Hawaii. While State Farm appreciates the need to protect consumers, the variation in privacy laws across the states presents operational challenges and may create confusion for consumers. For this reason, State Farm favors the enactment of a pre-emptive national data privacy law over the current patchwork of federal and state privacy requirements.

For the reasons set for above, we respectfully ask the Committee to Vote No on S.B. 974. Alternatively, if the Legislature is inclined to move forward with the legislation, State Farm proposes the following amendment to S.B. 974 to clarify that the proposed bill does not apply to insurers, the affiliates, or subsidiaries:

**Amend § -2 Scope; exemptions at pg. 11, Line 1 by adding:**

(4) financial institution or an affiliate of a financial institution, subject to the Gramm-Leach-Bliley Act, P.L. 106-102, and regulations adopted to implement that Act.

**Amend § -2 Scope; exemptions, pg. 11, Lines 5-6:**

(2) ~~Nonpublic personal~~ Information collected, processed, sold or disclosed under and in accordance with as defined in the Gramm-Leach-Bliley Act (15 U.S.C. chapter 94) and regulations adopted to implement that Act;

**Amend § -3 Personal data rights; consumers, pg. 16, Line 13:**

Delete the word “insurance” from the provision that allows consumers to “opt-out” of processing of personal data to align with the GLBA exemption.

Thank you for the opportunity to submit testimony.



**SanHi**

GOVERNMENT STRATEGIES

A LIMITED LIABILITY LAW PARTNERSHIP

DATE: February 21, 2023

TO: Senator Donovan Dela Cruz  
Chair, Committee on Ways and Means

FROM: Mihoko E. Ito

RE: **S.B. 974, S.D. 1, Relating to Consumer Data Protection**  
**Hearing Date: February 22, 2023 at 9:30 a.m.**  
**Conference Room 211 & Videoconference**

---

Dear Chair Dela Cruz, Vice Chair Keith-Agaran, 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 respectfully **submits comments** regarding S.B. 974, Relating to Consumer Data Protection, which establishes a framework to regulate controllers and processors with access to personal consumer data, establishes penalties and appropriates funds to carry out enforcement of the proposed law.

We appreciate that this measure is aimed at addressing privacy in a comprehensive manner, but are concerned that the bill might be difficult for businesses to comply with as currently drafted. For financial institutions, we would note that this bill does contain a Gramm Leach Bliley Act (GLBA) exemption, which typically covers personal information that is collected by financial institutions. However, in its current form, the bill only covers "nonpublic personal information" as defined in the Gramm-Leach-Bliley Act. As noted by other testifiers, we believe that this definition needs to be expanded to specifically include financial institutions, including affiliates that are subject to the GLBA.

Finally, we would suggest that, with the many complexities of this bill and significant impact on business operations, it is imperative to discuss these details with stakeholders to make sure that the obligations are workable and do not result in unintended consequences.

Thank you for the opportunity to submit this testimony.

# HAWAII FINANCIAL SERVICES ASSOCIATION

c/o Marvin S.C. Dang, Attorney-at-Law

P.O. Box 4109

Honolulu, Hawaii 96812-4109

Telephone No.: (808) 521-8521

February 22, 2023

Senator Donovan M. Dela Cruz, Chair  
Senator Gilbert S.C. Keith-Agaran, Vice Chair  
and members of the Senate Committee on Ways and Means  
Hawaii State Capitol  
Honolulu, Hawaii 96813

Re: **S.B. 974, S.D. 1 (Consumer Data Protection)**  
**Decision Making Date/Time: Wednesday, February 22, 2023, 9:30 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: establishes a framework to regulate controllers and processors with access to personal consumer data; establishes penalties; establishes a new consumer privacy special fund; and appropriates moneys.

We recommend that this Bill be amended in Sec. -2(b) (Scope; exemptions), which is on page 10, line 19 through page 11, line 1, to add in (4):

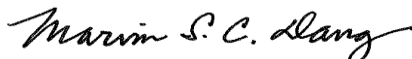
- (b) This chapter shall not apply to any:
- (1) Government entity;
  - (2) Nonprofit organization;
  - (3) Institution of higher education; or
  - (4) Financial institution or an affiliate of a financial institution as defined by and that is subject to the federal Gramm-Leach-Bliley Act, 15 U.S.C. Sec. 6801 et seq., as amended, and implementing regulations, including Regulation P, 12 C.F.R. 1016.**

This type of exemption for a financial institution, including an affiliate, that is subject to the Gramm-Leach-Bliley Act, would “level the playing field” and is based on recently enacted Colorado (2021) and Utah (2022) privacy statutes. Additionally, the concept of an exemption for a financial institution that is subject to GLBA is in H.B. 1497, House Draft 1 (Consumer Data Protection) on page 9, lines 15-18.

The HFSA and other organizations had proposed this exemption in written testimony when this Bill was heard by the Senate Commerce & Consumer Protection (CPN) Committee on February 10, 2023. Additionally, at the CPN hearing, various organizations proposed other types of amendments which weren’t incorporated into the Senate Draft 1.

**Because of the complexity of this Bill, perhaps it should be deferred to allow interested parties to work on a comprehensive privacy legislation during the interim before the 2024 legislative session. That approach would be similar to the approach being taken on S.B. 1085 (Biometric Information Privacy) and S.B. 1180 (Privacy).**

Thank you for considering our testimony.



MARVIN S.C. DANG

Attorney for Hawaii Financial Services Association

To:            The Honorable Donovan M. Dela Cruz, Chair  
                  The Honorable Gilbert S.C. Keith-Agaran, Vice Chair  
                  Senate Committee on Ways and Means

From:         Mark Sektnan, Vice President

Re:            **SB 974 SD1 – Relating to Consumer Data Protection**  
                  **APCIA Position: Request for Amendments**

Date:         Wednesday, February 22, 2023  
                  9:30 a.m., Conference Room 211 & Videoconference

Aloha Chair Dela Cruz, Vice Chair Keith-Agaran and Members of the Committee:

The American Property Casualty Insurance Association of America (APCIA) is **requesting amendments to SB 974 SD1** related to data privacy. The American Property Casualty Insurance Association (APCIA) is the primary national trade association for home, auto, and business insurers. APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers, with a legacy dating back 150 years. APCIA members represent all sizes, structures, and regions—protecting families, communities, and businesses in the U.S. and across the globe.

APCIA appreciates the author’s intention to protect the private information of people living in Hawaii. Section 2 (c) (2) exempts insurers who are already covered by the Graham-Leach-Bliley Act of 1999 but should be expanded to allow exempt the entity level companies per the following language:

- Provided further, nothing in this act shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder.

APCIA would also suggest that Section 2, subsection (b), of the bill should be expanded to exempt those insurers licensed under Chapters 431 and 432, Hawaii Revised Statutes, because the Data Security Model Law as proposed by the National Association of Insurance Commissioners (NAIC) was adopted in Hawaii in 2021 and is now codified as Article 3B, Chapter 431, Hawaii Revised Statutes. This NAIC model law was specifically drafted by the NAIC for the property and casualty insurance industry (and health insurers) to properly manage and secure personal information.

For these reasons, APCIA asks the committee to **amend** this bill in committee.



**LATE**

February 23, 2023

Chair Donovan M. Dela Cruz  
Vice Chair Gilbert S.C. Keith-Agaran  
Committee on Ways and Means  
Hawaii State Senate  
415 South Beretania Street  
Honolulu, HI 96817

**Re: SB 974, Hawaii Consumer Privacy Legislation - SUPPORT IF AMENDED**

Dear Chair Chair Dela Cruz, Vice Chair Keith-Agaran, and Members of the Committee on Ways and Means,

Consumer Reports<sup>1</sup> sincerely thanks you for your work to advance consumer privacy in Hawaii. SB 974 would extend to Hawaii consumers important new protections, including the right to know the information companies have collected about them, the right to access, correct, and delete that information, as well as the ability to require businesses to honor authorized agents' browser privacy signals as an opt out of sale, targeted advertising, and profiling.

Consumers currently possess very limited power to protect their personal information in the digital economy, while online businesses operate with virtually no limitations as to how they process that information (so long as they note their behavior somewhere in their privacy policy). As a result, consumers' every move is constantly tracked and often combined with offline activities to provide detailed insights into their most personal characteristics, including health conditions, political affiliations, and sexual preferences. This information is sold as a matter of course, is used to deliver targeted advertising, facilitates differential pricing, and enables opaque algorithmic scoring—all of which can lead to disparate outcomes along racial and ethnic lines.

At the same time, spending time online has become integral to modern life, with many individuals required to sign-up for accounts with tech companies because of school, work, or simply out of a desire to connect with distant family and friends. Consumers are offered the illusory "choice" to consent to company data processing activities, but in reality this is an all or

---

<sup>1</sup> Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

nothing decision; if you do not approve of any one of a company's practices, you can either forgo the service altogether or acquiesce completely.

While we prefer privacy legislation that limits companies' collection, use, and disclosure of data to what is reasonably necessary to operate the service (i.e. data minimization)<sup>2</sup> or that at least restricts certain types of processing (sales, targeted advertising, and profiling), we appreciate that SB 974 creates a framework for universal opt-out through universal controls and authorized agents. Strong data minimization provisions are our first choice because they prevent consumers from constantly operating from a defensive position where they must determine whether each company that they interact with performs processing activities they consider acceptable or not. However, privacy legislation with universal opt-outs also empowers consumers by making it easier to manage the otherwise untenably complicated ecosystem of privacy notices, opt-out requests, and verification.<sup>3</sup> The goal of universal opt-out is to create an environment where consumers can set their preference once and feel confident that businesses will honor their choices as if they contacted each business individually.

Measures largely based on an opt-out model with no universal opt-out, like the original interpretation of the California Consumer Privacy Act (CCPA), would require consumers to contact hundreds, if not thousands, of different companies in order to fully protect their privacy. Making matters worse, Consumer Reports has documented that some CCPA opt-out processes are so onerous that they have the effect of preventing consumers from stopping the sale of their information.<sup>4</sup>

Sections 3(b) and 4 of the bill requires that covered businesses allow consumers or their authorized agents to opt-out from a controller's processing of personal data for the purpose of targeted advertising, sales, and profiling. Privacy researchers, advocates, and publishers have already created multiple technologies that would fit the bill for an authorized agent under this draft, including the Global Privacy Control (GPC)<sup>5</sup> and Consumer Reports' own Permission Slip<sup>6</sup>, both of which could help make the opt-out model more workable for consumers.

Section 8 also provides key assurances that controllers truly deidentify data if they are to rely on the "deidentified data" exception to the definition of "personal data." The section requires that controllers commit to maintaining and using deidentified data without attempting to reidentify it

---

<sup>2</sup> Section 5(a)(1) of the bill ostensibly includes data minimization language; however, because data processing is limited to any purpose listed by a company in its privacy policy — instead of to what is reasonably necessary to fulfill a transaction — that language will in practice have little effect.

<sup>3</sup> Aleecia M. McDonanld and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society*, vol. 4, no. 3 (2008), 543-568.

[https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP\\_V4N3\\_543.pdf?sequence=1&isAllowed=y](https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf?sequence=1&isAllowed=y)

<sup>4</sup> Maureen Mahoney, California Consumer Privacy Act: Are Consumers' Rights Protected, *CONSUMER REPORTS* (Oct. 1, 2020),

[https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR\\_CCPA-Are-ConsumersDigital-Rights-Protected\\_092020\\_vf.pdf](https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-ConsumersDigital-Rights-Protected_092020_vf.pdf).

<sup>5</sup> Global Privacy Control, <https://globalprivacycontrol.org>.

<sup>6</sup> Ginny Fahs, Introducing Permission Slip, the app to take back control of your data, *Consumer Reports* (Nov. 16, 2022), <https://digital-lab-wp.consumerreports.org/2022/11/16/introducing-permission-slip/>

later on and that the controller enter into and monitor contracts with any recipient of deidentified data so that the recipient is held to the controller's own obligations under the legislation. Privacy legislation too often allows controllers to shirk their responsibilities through weak definitions of deidentification that fail to truly protect consumer privacy by allowing the trivial reidentification of personal data.

However, the legislation still contains significant loopholes that would hinder its overall effectiveness. We offer several suggestions to strengthen the bill to provide the level of protection that Hawaiians deserve.

- *Broaden opt-out rights to include all data sharing and ensure targeted advertising is adequately covered.* SB 974's opt out should cover all data transfers to a third party for a commercial purpose (with narrowly tailored exceptions). In California, many companies have sought to avoid the CCPA's opt out requirements by claiming that much online data sharing is not technically a "sale" (appropriately, CPRA expands the scope of California's opt-out to include all data sharing and clarifies that targeted ads are clearly covered by this opt out).<sup>7</sup> We recommend the following definition:

*"Share" [or sell] means renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration, or otherwise for a commercial purpose.*

While we appreciate that this measure has an opt out for targeted advertising, the current definition of targeted advertising is ambiguous, and could allow internet giants like Google, Facebook, and Amazon to serve targeted ads based on their own vast data stores on other websites. This loophole would undermine privacy interests and further entrench dominant players in the online advertising ecosystem. We recommend using the following definition:

*"Targeted advertising" means the targeting of advertisements to a consumer based on the consumer's activities with one or more businesses, distinctly-branded websites, applications or services, other than the business, distinctly branded website, application, or service with which the consumer intentionally interacts. It does not include advertising: (a) Based on activities within a controller's own commonly-branded websites or online applications; (b) based on the context of a consumer's current search query or visit to a website or online application; or (c) to a consumer in response to the consumer's request for information or feedback.*

---

<sup>7</sup> Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously*, *supra* note 3, Medium (January 9, 2020), <https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb>.



- *Tighten the definition and interpretation of bona fide loyalty programs to eliminate loopholes.* We are concerned that the draft legislation’s exception to the anti-discrimination provision when a consumer voluntarily participates in a “bona fide reward, club card or loyalty program” is too vague and could offer companies wide loopholes to deny consumer rights by simply labeling any data sale or targeted advertising practice as part of the “bona fide loyalty program.” We urge the drafters to adopt a more precise definition and to provide clearer examples of prohibited behavior that does not fall under this exception. For example, it’s reasonable that consumers may be denied participation in a loyalty program if they have chosen to delete information or deny consent for processing functionally necessary to operate that loyalty program. That is, if you erase a record of having purchased nine cups of coffee from a vendor, you cannot expect to get the tenth cup for free. However, generally controllers do not need to sell data to others or to engage in cross-site targeted advertising in order to operate a bona fide loyalty program — such behaviors have nothing to do with the tracking of purchases to offer discounts or first-party advertising.
- *Limit authentication requirements to request to access, correct, and delete.* Section 3(a) allows controllers to authenticate consumer requests to exercise any of their rights under the act. This may be appropriate when consumers are requesting to access, delete, or correct their information, since fraudulent requests for these rights can pose real consumer harm. However, opt out rights do not carry similar risks to consumers and therefore should not be subjected to this heightened standard. In the past, businesses have used authentication clauses to stymie rights requests by insisting on receiving onerous documentation.<sup>8</sup> For example, in Consumer Reports’s investigation into the usability of new privacy rights in California, we found examples of companies requiring consumers to fax in copies of their drivers’ license in order to verify residency and applicability of CCPA rights.
- *Apply authorized agent provisions to rights to access, correct, and delete.* SB 974 currently only allows authorized agents to send requests to opt out, meaning for all other rights requests consumers must go to each business they interact with one by one and navigate its bespoke system. This means requests to access, correct, and delete are impractical to use at scale, especially when the law allows businesses to ask for onerous documentation to complete the request. The purpose of authorized agents is to cut down on the amount of time that each consumer must spend haggling with individual businesses to accept their rights requests, ultimately making those rights much more usable for consumers. CPRA and Oregon’s SB 619 currently include a similar provision.<sup>9</sup>
- *Remove the right to cure from the Attorney General enforcement section.* The “right to cure” provisions from the administrative enforcement sections of the bill should be

---

<sup>8</sup> Ibid.

<sup>9</sup> See California Civil Code 1798.130 A(3)(a), <https://cpa.gtlaw.com/cpra-full-text/>



removed — as Proposition 24 removed similar provisions from the CCPA.<sup>10</sup> In practice, the “right to cure” is little more than a “get-out-of-jail-free” card that makes it difficult for the AG to enforce the law by signaling that a company won’t be punished the first time it’s caught breaking the law.

- *Include strong civil rights protections.* A key harm observed in the digital marketplace today is the disparate impact that can occur through processing of personal data for the purpose of creating granularized profiles of individuals based off of data both collected and inferred about them. Therefore a crucial piece of strong privacy legislation is ensuring that a business’ processing of personal data does not discriminate against or otherwise makes opportunity or public accommodation unavailable on the basis of protected classes. A number of privacy bills introduced federally in recent years have included such civil rights protections, including the American Data Privacy and Protection Act which overwhelmingly passed the House Energy and Commerce Committee on a 53-2 bipartisan vote.<sup>11</sup> Consumer Reports’ Model State Privacy Legislation also contains specific language prohibiting the use of personal information to discriminate against consumers.<sup>12</sup>

Thank you again for your consideration, and for your work on this legislation. We look forward to working with you to ensure that Hawaii residents have the strongest possible privacy protections.

Sincerely,  
Matt Schwartz  
Policy Analyst

---

<sup>10</sup> At the very least, the right to cure should sunset like it does under the Connecticut Data Privacy Act. See Public Act No. 22-15, Section 11(b), <https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF>

<sup>11</sup> See Section 2076, Amendment in the Nature of a Substitute to the American Data Privacy and Protection Act, <https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-117-8152-P000034-Amdt-1.pdf>

<sup>12</sup> See Sections 125 and 126, Consumer Reports, Model State Privacy Act, (Feb. 2021) [https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR\\_Model-State-Privacy-Act\\_022321\\_vf.pdf](https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf)

**SB-974-SD-1**

Submitted on: 2/20/2023 7:41:37 PM

Testimony for WAM on 2/22/2023 9:30:00 AM

<b>Submitted By</b>	<b>Organization</b>	<b>Testifier Position</b>	<b>Testify</b>
Hunter Heavilin	Individual	Support	Written Testimony Only

Comments:

As the world becomes increasingly digital, it is more important than ever to protect the privacy and security of consumers' personal information. The amount of personal data that is collected, stored, and shared by companies is growing at an exponential rate, and it is crucial that we establish a framework to regulate the handling of this information.

SB974, the Consumer Data Protection bill, takes important steps towards this goal by establishing a framework to regulate the handling of personal consumer data by controllers and processors. This bill will help ensure that companies are transparent about what data they are collecting, how they are using it, and who they are sharing it with. Additionally, by establishing penalties for non-compliance, this bill will provide consumers with recourse in the event that their personal data is misused. The establishment of the consumer privacy special fund is a critical step towards ensuring that the resources are available to enforce the provisions of this bill and protect consumers' privacy rights.