JOSH GREEN, M.D.
GOVERNOR | KE KIA'ĀINA

SYLVIA LUKE
LIEUTENANT GOVERNOR | KA HOPE KIA'ĀINA

STATE OF HAWAII | KA MOKUʻĀINA ʻO HAWAIʻI
OFFICE OF THE DIRECTOR
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS
KA ʻOIHANA PILI KĀLEPA
335 MERCHANT STREET, ROOM 310
P.O. BOX 541
HONOLULU, HAWAII 96809
Phone Number: 1-844-808-DCCA (3222)
Fax Number: (808) 586-2856
cca.hawaii.gov

NADINE Y. ANDO
DIRECTOR | KA LUNA HOʻOKELE

DEAN I. HAZAMA
DEPUTY DIRECTOR | KA HOPE LUNA HOʻOKELE

Testimony of the Department of Commerce and Consumer Affairs

Before the
Senate Committee on Labor and Technology
Friday, January 30, 2026
3:00 p.m.
Via Videoconference
and
Conference Room 225

On the following measure:
S.B. 1163, RELATING TO PRIVACY

Chair Elefante and Members of the Committee:

My name is Radji Tolentino, and I am an Enforcement Attorney with the Department of Commerce and Consumer Affairs' Office of Consumer Protection. The Department appreciates the intent of, and offers comments on, this bill.

The purpose of this bill is to prohibit the sale of geolocation information and internet browser information without consent and prohibits the sale of data collected through eavesdropping or through an application operating in the background of a device that uses the device's microphone.

OCP supports the intent of S.B. 1163. Protecting consumers' personal data, such as geolocation and browsing history, is very important. The unregulated sale of this information poses real risks to privacy and safety. The Federal Trade Commission highlighted consumer harms in its enforcement action against a data broker selling

geolocation information that could be used to track an individual's proximity to an abortion clinic. OCP feels that stronger safeguards are needed.

However, these protections would be more effective as part of a comprehensive data privacy law rather than a standalone prohibition. Nineteen states have already adopted comprehensive privacy laws that set uniform standards for how personal data is collected, used, and sold, and when and how consumers can opt-out of the collection and sale of their data. These laws address sensitive data like geolocation while providing clarity for consumers, businesses, and enforcement agencies.

This bill codifies the new law in Chapter 481B, which means a violation would constitute an Unfair or Deceptive Act or Practice (UDAP) under Hawaii's consumer protection law and would be enforceable by a consumer, the Attorney General or OCP. However, OCP currently lacks specialized expertise in geolocation technologies, mobile data collection, data brokers, and the technologies used and misused in privacy violations.

Many states with comprehensive privacy laws have dedicated enforcement resources, including technologists or privacy specialists, who play a critical role in effective privacy enforcement. These experts analyze how companies collect, use, and transfer data through applications, APIs, and background processes. They help investigators understand complex data flows and assess whether data can be re-identified, evaluate compliance with consent requirements and data minimization obligations, support investigations involving data brokers, location tracking, and emerging technologies and translate technical data practices into clear, usable evidence for enforcement actions and litigation.

Without this expertise, enforcement agencies may struggle to identify violations, assess risks, and hold sophisticated actors accountable. This is particularly true when dealing with large-scale data collection.

For these reasons, OCP recommends addressing geolocation and other sensitive data protections through a comprehensive state privacy law. A comprehensive approach would also modernize the definition of "personal information," address emerging privacy issues, and ensure enforcement agencies have the appropriate resources.

If this committee decides to proceed with a comprehensive data privacy bill, we respectfully suggest forming a task force composed of key stakeholders that would meet to develop a bill that addresses the needs of both Hawaii consumers and enforcement agencies.

Thank you for the opportunity to testify on this bill.

DEPARTMENT OF THE PROSECUTING ATTORNEY
KA ʻOIHANA O KA LOIO HOʻOPIʻI
CITY AND COUNTY OF HONOLULU

ALII PLACE
1060 RICHARDS STREET • HONOLULU, HAWAIʻI 96813
PHONE: (808) 768-7400 • FAX: (808) 768-7515 • WEB: https://honoluluprosecutor.org/

STEVEN S. ALM
PROSECUTING ATTORNEY
LOIO HOʻOPIʻI

THOMAS J. BRADY
FIRST DEPUTY PROSECUTING ATTORNEY
HOPE MUA LOIO HOʻOPIʻI

THE HONORABLE BRANDON J.C. ELEFANTE, CHAIR
SENATE COMMITTEE ON LABOR AND TECHNOLOGY
Thirty-Third State Legislature
Regular Session of 2026
State of Hawai`i

January 29, 2026

RE: S.B. 1163; RELATING TO PRIVACY.

Chair Elefante, Vice Chair Lamosao, and members of the Senate Committee on Labor and Technology, the Department of the Prosecuting Attorney of the City and County of Honolulu submits the following testimony in **support** of S.B. 1163 **with a recommended amendment**.

S.B. 1163 broadly prohibits the sale of geolocation information and Internet browser information without consent. It also prohibits covert eavesdropping through background computer applications.

The Department shares many of the concerns about privacy raised in this bill. Data brokerages can facilitate harassment, stalking, and abuse.[1] The assassination of Minnesota representative Melissa Hortman and her husband was apparently aided by information bought from data brokers.[2] Black market data brokers can even sell the information collected on American to foreign adversaries, a clear threat to national security.[3]

The Department respectfully recommends an exemption for lawful investigation by the police. These investigations must scrupulously comply with both constitutional and statutory privacy protections. The Hawai‘i Supreme Court has held that voluntary disclosure of personal information to a third party does necessarily not relinquish a reasonable expectation of privacy.[4] Thus, even when seeking information from third-party vendors, police usually require a warrant.

---

[1] *See generally* Thomas E. Kadri, *Brokered Abuse*, 3 J. FREE SPEECH L. 137 (2023), *available at* https://digitalcommons.law.uga.edu/fac_artchop/1571.
[2] MEPRISM PRIVACY, *The Minnesota Political Assassination Plot: A Chilling Case Study*, *available at* https://meprism.com/blog/how-data-brokers-enable-political-violence.
[3] NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, *Data Brokers and Security: Risks and Vulnerabilities Related to Commercially Available Data*, *available at* https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf.
[4] *State v. Walton*, 133 Hawai‘i 66, 91-100, 324 P.3d 876, 901-10 (2014).

Hawai‘i law permits seizure of electronic data pursuant to a search warrant.[5] With special judicial authorization, law enforcement may also conduct wiretaps or intercept live electronic data.[6] These investigative tools are critical to prosecuting serious criminal offenses such as murder, kidnapping, sexual assault, child pornography, and organized crime. In some cases, police might consult with private vendors who have the requisite technical ability.

Legitimate commercial databases also provide police with important leads. For example, the National Insurance Crime Bureau provides no-cost support to law enforcement in combatting insurance fraud and theft rings.[7] Likewise, some commercial databases can supply clues for finding and apprehending fugitives.

Given a narrow exception for legitimate existing law enforcement purposes, the Department supports this measure.

Thank you for the opportunity to testify.

[5] HRS Chapter 803, Part III.
[6] HRS Chapter 803, Part IV.
[7] NATIONAL INSURANCE CRIME BUREAU, *available at* https://www.nicb.com/law-enforcement.

January 29, 2026

Senator Henry J.C. Aquino
Chair, Senate Committee
on Labor and Technology
Hawaii State Capitol, Room 204
Honolulu, HI 96813

Senator Chris Lee
Vice Chair, Senate Committee
on Labor and Technology
Hawaii State Capitol, Room 219
Honolulu, HI 96813

RE: Letter in Opposition to Hawaii SB 1163

Dear Chair Aquino and Vice Chair Lee:

On behalf of the advertising industry, we write to oppose Hawaii SB 1163.[1] We provide this letter to offer our non-exhaustive list of concerns about this bill. SB 1163 would ban routine uses of browser information without consent and deviate from typical data privacy legislation by providing no exceptions. Accordingly, we ask you to decline to advance the bill as drafted out of the Senate Committee on Labor and Technology ("Committee"). The bill would impede the ad-subsidization of the Internet for Hawaiians, increasing the cost for access to web-based and app-based services, because the bill's language inadvertently limits responsible digital advertising.[2]

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country. These companies range from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,000 companies that power the commercial Internet, which accounted for nearly 20 percent of total U.S. gross domestic product ("GDP") in 2024.[3] By one estimate, approximately 17.5% of Hawaii jobs in 2024 were related to the ad-subsidized Internet, a share projected to increase to 19.3% by 2029.[4] Our group has more than a decade's worth of hands-on experience it can bring to bear on matters related to consumer privacy and controls. We would welcome the opportunity to engage with the Committee further on the points we discuss in this letter.

I. SB 1163 would substantially disrupt Internet commerce by mandating an opt-in consent framework that goes far beyond every other state privacy law.

SB 1163 would require explicit consumer consent for any sale or offering for sale of "internet browser information," defining "sale" so broadly that it would encompass nearly any transfer of such data to another business or third party for monetary or other valuable consideration.[5] This would result in an isolated, local marketplace where Hawaiians are inundated with repeat consent requests for routine online activities, creating notice fatigue and

---

[1] Hawaii SB 1163 (2025-2026 Session), located here (hereinafter, "SB 1163").
[2] *See* Digital Advertising Alliance, *Americans Value Free Ad-Supported Online Services at $1,400/Year; Annual Value Jumps More than $200 Since 2016* (Sept. 28, 2020), located here.
[3] S&P Global, THE ECONOMIC IMPACT OF ADVERTISING ON THE US ECONOMY, 2024-2029 at 4 (Aug. 2025), located at https://theadcoalition.com/wp-content/uploads/2025/08/TAC_SP-Global-Final-Report_August-2025.pdf.
[4] *Id.* at 15-16.
[5] SB 1163 § 2.

significant frustration, while fundamentally changing how Hawaiians access the products and services they rely on through the Internet. This consent-based approach has been tried in other countries and led to widespread consumer fatigue and frustration.

As drafted, SB 1163 would adopt a privacy framework that is out of step with approaches taken by other states, undermine the ad-supported Internet, and disrupt the online marketplace. Data transfers are essential to digital advertising, which supports the broader economy and allows publishers, hotels, airlines, farmers, fruit producers, and myriad other industries to provide content, news, and services for free or at low cost to consumers. Small and mid-sized businesses rely on the very form of digital advertising that this bill would stymie.[6] The opt-in consent requirement in SB 1163 threatens to dismantle this ecosystem, which benefits small businesses and Hawaiian consumers alike. We therefore respectfully urge you to remove the consent requirement for "sales" of "internet browser information" from the bill.

II. SB 1163 should be harmonized with other state privacy laws to foster consistency and clarity for consumers and businesses.

If enacted, SB 1163 would make the state's approach to privacy an outlier in ways that would harm Hawaiians and businesses of all sizes. For example, SB 1163 diverges from other states' consumer privacy regimes and proposals, such as the California Consumer Privacy Act and others, which grant consumers a right to opt out of personal information sales rather than imposing an opt-in consent regime. SB 1163's proposed opt-in consent requirement for internet browser information threatens to impede basic internet functions, such as rendering webpages and allowing Hawaiians to connect with digital products, services, and content.

In addition, SB 1163 omits widely adopted exceptions included in other data privacy laws across the country, including exceptions for fraud prevention, fulfilling consumer requests for products and services (e.g., mapping applications or suggesting the nearest gas station), and compliance with existing laws such as the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act, among others. As a result, many routine and expected data transfers would be treated as prohibited "sales." This is particularly a concern with respect to the bill's proposed restrictions on sale of geolocation data, which is a vital signal in combatting fraud against consumers as well as helping them find their way, for example, to local eateries along hiking trails and myriad other routine and expected uses. We encourage the Committee to focus its efforts on harmonizing the bill with the approach to privacy in the majority of other states. Efforts to harmonize state privacy legislation with existing privacy laws are critical to minimizing costs of compliance and fostering similar privacy rights for consumers no matter where they live. If enacted, SB 1163 would subject Hawaiians to an entirely different, and drastically more limited, Internet experience than consumers in other states.

In addition, compliance costs associated with divergent privacy laws are significant. To make the point: a regulatory impact assessment of the California Consumer Privacy Act of 2018

---

[6] *See* Digital Advertising Alliance, *Summit Snapshot: Data Drives Small- and Mid-sized Business Online, It's Imperative that Regulation not Short-Circuit Consumer Connections* (Aug. 17, 2021), located here.

concluded that the initial compliance costs to California firms would be $55 billion.[7] Another recent study found that a consumer data privacy proposal in a different state considering privacy legislation would have generated a direct initial compliance cost of $6.2 billion to $21 billion and ongoing annual compliance costs of $4.6 billion to $12.7 billion for the state.[8] Other studies confirm the staggering costs associated with varying state privacy standards. One report found that state privacy laws could impose out-of-state costs of between $98 billion and $112 billion annually, with costs exceeding $1 trillion dollars over a 10-year period, and with small businesses shouldering a significant portion of the compliance cost burden.[9] Hawaii should not add to this compliance bill for businesses and should instead opt for an approach to data privacy that is in harmony with the majority of existing state privacy laws.

* * *

[7] *See* State of California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations*, 11 (Aug. 2019), located at https://dof.ca.gov/media/docs/forecasting/economics/major-regulations/major-regulations-table/CCPA_Regulations-SRIA-DOF.pdf.

[8] *See* Florida Tax Watch, *Who Knows What? An Independent Analysis of the Potential Effects of Consumer Data Privacy Legislation in Florida*, 2 (Oct. 2021), located at https://floridataxwatch.org/DesktopModules/EasyDNNNews/DocumentDownload.ashx?portalid=210&moduleid=34407&articleid=19090&documentid=986.

[9] Daniel Castro, Luke Dascoli, and Gillian Diebold, *The Looming Cost of a Patchwork of State Privacy Laws* (Jan. 24, 2022), located at https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws (finding that small businesses would bear approximately $20-23 billion of the out-of-state cost burden associated with state privacy law compliance annually).

We respectfully ask the Committee not to advance SB 1163, as its provisions would negatively affect both businesses and consumers alike. Rather than strengthening consumer protections, the bill would deal a substantial blow to the online economy, limiting businesses' ability to responsibly use data to offer Hawaiians access to the products, services, and online experiences they expect and enjoy.

Thank you in advance for your consideration of this letter.

Sincerely,

Christopher Oswald
EVP for Law, Ethics & Govt. Relations
Association of National Advertisers
202-296-1883

Alison Pepper
EVP, Government Relations & Sustainability
American Association of Advertising Agencies, 4As
202-355-4564

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

Lou Mastria
CEO
Digital Advertising Alliance
347-770-0322

CC: Members of the Hawaii Senate Committee on Labor and Technology

Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP
Matthew Stern, Venable LLP

Hawaiian Telcom

Written Statement of

Jeannine Souki,
Senior Manager – Government & Regulatory Affairs

SENATE COMMITTEE ON LABOR & TECHNOLOGY
January 30, 2026, 10 AM
State Capitol, Conference Room 225 & Videoconference

COMMENTS AND REQUEST TO AMEND:

SB 1163 – RELATING TO PRIVACY

To: Chair Elefante, Vice Chair Lamosao, and Members of the Committee
Re: Testimony providing comments with request for an amendment to SB1163

Aloha Honorable Chair, Vice-Chair, and Members of the Committee:

Mahalo for the opportunity to provide **comments for SB1163, Relating to Privacy**, with a **requested clarifying amendme**nt related to federally regulated telecommunications privacy requirements.

SB1163 seeks to protect consumers by prohibiting the sale of sensitive geolocation and internet browser information without consent. Hawaiian Telcom supports the bill's underlying goal of safeguarding customer privacy and preventing misuse of sensitive data.

However, we respectfully request a **narrow, technical amendment** to clarify that the bill does **not** apply to **Customer Proprietary Network Information (CPNI)** already governed by **federal law**. Telecommunications carriers are subject to comprehensive and longstanding privacy obligations under **Section 222 of the federal Communications Act** and **FCC regulations**, which strictly regulate the use, disclosure, and protection of CPNI, including location-related call information.

Without an explicit exemption, SB1163 could unintentionally create **overlapping or conflicting requirements** for telecommunications carriers that are already fully regulated at the federal level. Many states address this issue by expressly exempting data and entities regulated under federal CPNI rules to ensure regulatory consistency and avoid duplicative compliance obligations.

Requested Amendment:
Add a provision clarifying that SB1163 does not apply to:
Customer Proprietary Network Information (CPNI), as defined and regulated under federal law, or to telecommunications carriers to the extent they are acting in compliance with applicable federal CPNI requirements.

This amendment would preserve the bill's intent while ensuring alignment with federal law and avoiding unintended consequences for regulated telecommunications providers.

For these reasons, **Hawaiian Telcom supports SB1163 with the requested amendment** and respectfully urges your committee to adopt this clarification.

Mahalo for your consideration.

STATE PRIVACY & SECURITY COALITION

January 29, 2026

The Honorable Brandon J.C. Elefante, Chair
The Honorable Rachele Lamosao, Vice Chair
Senate Committee on Labor and Technology
Hawaii State Senate
415 South Beretania Street
Honolulu, HI 96817

Re: SB 1163 – Precise Location Data, Internet Browser Information, Etc.

Dear Chair Elefante, Vice Chair Lamosao, and Members of the Committee:

The State Privacy & Security Coalition (SPSC), a coalition of over 30 companies and seven trade associations in the retail, technology, telecommunications, payment card, and healthcare sectors, appreciates the opportunity to provide testimony on SB 1163. Protecting consumers from misuse of sensitive data is a critical priority, and SPSC recognizes the importance of ensuring strong safeguards for information such as precise geolocation data. We must respectfully urge the Committee to defer SB 1163 due to significant concerns about the bill's fragmented regulatory structure and the unintended consequences such an approach would create.

SB 1163 regulates discrete categories of data through standalone statutory restrictions rather than through a comprehensive privacy framework governing the collection, use, and disclosure of personal data across contexts. By focusing on individual data elements such as geolocation information, internet browser information, and certain audio-derived data, the bill risks creating a statutory model that would require repeated legislative updates as technologies and data uses evolve. In contrast, modern state privacy statutes establish consistent consumer rights and business obligations across categories of personal data while allowing scalable and durable compliance programs.

Similar versions of SB 1163 have been introduced in prior legislative sessions. As a result, the bill relies on terminology that does not align with definitions now commonly used across multi-state privacy frameworks, which may create consumer confusion and reduce interoperability across jurisdictions. For example:

- **Precise Geolocation**: "Precise geolocation data" is typically defined using a 1,750-foot radius threshold. The bill instead defines "precise location" using a one-mile radius, expanding the category of regulated data beyond the scope typically covered under multi-state privacy statutes.

- **Consent**: Consent is generally defined as a clear, affirmative, freely given, specific, informed, and unambiguous agreement, and excludes passive acceptance, bundled consents, and dark-pattern-driven interactions. SB 1163 departs from the national consensus, increasing the risk of inconsistent interpretation and enforcement outcomes.

- **Sale**: Sale is generally defined as an exchange of personal data for monetary or other valuable consideration while preserving operational exclusions such as processor transfers,

consumer-directed disclosures, and certain affiliate sharing. While the bill uses a broader definition modeled on the California Consumer Privacy Act (CCPA), that definition's breadth has created significant compliance questions and operational uncertainty. This construction risks capturing routine data flows that other states intentionally exclude to preserve service functionality and consumer expectations.

These definitional standards also reflect how state privacy law has evolved in recent years, including through the adoption of heightened protections for sensitive data. States such as Virginia, Colorado, and Connecticut have enacted modern privacy statutes that provide strong consumer protections while supporting consistent implementation across jurisdictions. Core elements common across those laws include:

- Opt-in consent requirements for processing sensitive data, including precise geolocation data;
- Robust consumer rights, including access, deletion, correction, and portability;
- Rights to opt out of targeted advertising, sale of personal data, and certain profiling activities;
- Risk assessment requirements for high-risk processing activities; and
- Contractual accountability requirements governing downstream data use.

Taken together, the widely adopted national privacy framework addresses sensitive data risks, including misuse of precise geolocation and other location-based data, through integrated consumer rights, controller accountability, and risk-based governance requirements that apply across data types and technologies. These laws require organizations to assess foreseeable risks, implement proportionate safeguards, and document mitigation measures before engaging in higher-risk data processing. Because these obligations apply across categories of personal data, the national model provides more durable protection against misuse of sensitive location data while remaining adaptable to evolving technologies.

SPSC recognizes Hawaii's interest in protecting residents from misuse of sensitive data. SPSC remains committed to working with the Legislature on solutions that strengthen consumer protections while maintaining alignment with widely adopted state privacy models. For these reasons, SPSC respectfully urges the Committee to defer SB 1163 and instead consider advancing privacy legislation that provides strong protections for consumers while ensuring operational clarity and interstate interoperability.

Respectfully submitted,

Andrew A. Kingman
Counsel, State Privacy & Security Coalition

SB-1163
Submitted on: 1/27/2026 1:48:11 PM
Testimony for LBT on 1/30/2026 3:00:00 PM

Submitted By	Organization	Testifier Position	Testify
B.A. McClintock	Individual	Support	Written Testimony Only

Comments:

Please support this important bill. Mahalo.

TECHNET
THE VOICE OF AMERICAN INNOVATION

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

LATE

January 30, 2026

Senator Brandon J.C. Elefante
Chair, Committee on Labor and Technology
Hawaii State Capitol
415 South Beretania Street, Room 217
Honolulu, HI 96813

Senator Rachele Lamosao
Vice Chair, Committee on Labor and Technology
Hawaii State Capitol
415 South Beretania Street, Room 204
Honolulu, HI 96813

RE: SB 1163 (Lee) - Relating to Privacy - Oppose

Dear Chair Elefante, Vice Chair Lamosao, and Members of the Committee

On behalf of TechNet, we respectfully oppose SB 1163, which would prohibit the sale of geolocation and internet browsing data.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of American innovation by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes 100 dynamic American businesses ranging from startups to the most iconic companies on the planet and represents five million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

We share the Legislature's commitment to protecting sensitive personal information and limiting the misuse of location data, particularly where such data could reveal information about an individual's health care or other highly sensitive activities. However, as drafted, the bill is overly broad, unclear in key respects, and would produce significant unintended consequences across multiple industries without advancing a coherent privacy framework.

<u>A Piecemeal Approach Rather Than a Comprehensive Framework</u>
We are not opposed in principle to prohibitions on the sale of precise geolocation information, particularly where such restrictions are narrowly tailored and accompanied by appropriate definitions, exceptions, and enforcement mechanisms. Indeed, several states have adopted restrictions on the sale of precise geolocation data as part of comprehensive privacy laws.

However, those laws operate within well-defined frameworks that distinguish among data types, permissible uses, and covered entities. If Hawaii seeks to adopt similar protections, a comprehensive approach, such as a Connecticut-style privacy framework or a targeted data broker regime, would provide clearer guidance and more durable protections than the piecemeal approach reflected in this bill.

Scope Extends Far Beyond Telecommunications

Although the bill proposes bans on the sale of location data and internet browsing data, its implications are not limited to the telecommunications industry. The bill applies to any person that sells or offers such data for sale if it is recorded or collected through a mobile device or a location-based application. As a result, the bill would reach a broad range of actors across the digital ecosystem, including app developers, online platforms, data intermediaries, and the advertising industry.

This broad scope highlights the importance of careful policy development. Wide bans that aren't based on a thorough privacy framework may hinder legitimate data uses and lack clear, enforceable standards.

Overbreadth and Ambiguity in Additional Data Categories

The bill's stated legislative intent is to prevent the sale of location data, particularly data capable of revealing information about individuals' receipt of health care. Yet the bill extends far beyond that objective by also prohibiting the sale of "eavesdropping" data and data collected by background applications that use a device's microphone.

These terms are undefined and raise significant questions about the bill's scope. It is unclear what constitutes "eavesdropping" data, what categories of data collected by background applications are covered, and whether the prohibition extends beyond audio data to include unrelated functionality data. Depending on interpretation, the bill could encompass a wide range of information that has no connection to geolocation or health care.

Importantly, the regulation of these additional data types goes well beyond the bill's stated purpose, undermining the principle that statutory restrictions should be tailored to the harms they seek to address.

Unintended Consequences for Cybersecurity and Fraud Prevention

The bill's broad prohibitions would also have unintended consequences for cybersecurity and fraud prevention. In practice, geolocation and related signals are used by cybersecurity firms and organizations to detect anomalous activity, prevent account takeovers, and respond to threats in real time.

By severing the lawful flow of location data for security purposes, the bill would significantly weaken the tools available to security professionals. In effect, it would

require bad actors to consent to the sharing of the very information used to protect accounts and systems—an outcome that undermines both consumer protection and public safety.

Protecting sensitive location information is an important policy goal, and we appreciate the Legislature's focus on strengthening privacy safeguards. However, SB 1163, as drafted, adopts an overly broad and fragmented approach that extends far beyond its stated intent, lacks critical definitions and exceptions, and risks undermining legitimate security and data uses.

A more targeted framework—focused on the sale of precise geolocation data and aligned with comprehensive privacy or data broker models—would better balance privacy, security, and innovation.

For these reasons, we respectfully oppose the bill and urge the Legislature to consider a more coherent, evidence-based approach to regulating the sale of sensitive location data.

If you have any questions regarding our position, please contact Robert Boykin at rboykin@technet.org or 408.898.7145.

Sincerely,

Robert Boykin
Executive Director for California and the Southwest
TechNet

STATE PRIVACY & SECURITY COALITION

January 30, 2026

LATE

The Honorable Brandon J.C. Elefante, Chair
The Honorable Rachele Lamosao, Vice Chair
Senate Committee on Labor and Technology
Hawaii State Senate
415 South Beretania Street
Honolulu, HI 96817

Re: SB 1163 – Privacy; Geolocation Information; Eavesdropping; Internet Browser Information

Dear Chair Elefante, Vice Chair Lamosao, and Members of the Committee:

The State Privacy & Security Coalition (SPSC), a coalition of over 30 companies and seven trade associations in the retail, technology, telecommunications, payment card, and healthcare sectors, appreciates the opportunity to provide testimony on SB 1163. Protecting consumers from misuse of sensitive data is a critical priority, and SPSC recognizes the importance of ensuring strong safeguards for information such as precise geolocation data. We must respectfully oppose SB 1163 due to significant concerns about the bill's fragmented regulatory structure and the unintended consequences such an approach would create.

SB 1163 regulates discrete categories of data through standalone statutory restrictions rather than through a comprehensive privacy framework governing the collection, use, and disclosure of personal data across contexts. By focusing on individual data elements such as geolocation information, internet browser information, and certain audio-derived data, the bill risks creating a statutory model that would require repeated legislative updates as technologies and data uses evolve. In contrast, modern state privacy statutes establish consistent consumer rights and business obligations across categories of personal data while allowing scalable and durable compliance programs.

Similar versions of SB 1163 have been introduced in prior legislative sessions. As a result, the bill relies on terminology that does not align with definitions now commonly used across multi-state privacy frameworks, which may create consumer confusion and reduce interoperability across jurisdictions. For example:

- **Precise Geolocation**: "Precise geolocation data" is typically defined using a 1,750-foot radius threshold. The bill instead defines "precise location" using a one-mile radius, expanding the category of regulated data beyond the scope typically covered under multi-state privacy statutes.

- **Consent**: Consent is generally defined as a clear, affirmative, freely given, specific, informed, and unambiguous agreement, and excludes passive acceptance, bundled consents, and dark-pattern-driven interactions. SB 1163 departs from the national consensus, increasing the risk of inconsistent interpretation and enforcement outcomes.

- **Sale**: Sale is generally defined as an exchange of personal data for monetary or other valuable consideration while preserving operational exclusions such as processor transfers,

consumer-directed disclosures, and certain affiliate sharing. While the bill uses a broader definition modeled on the California Consumer Privacy Act (CCPA), that definition's breadth has created significant compliance questions and operational uncertainty. This construction risks capturing routine data flows that other states intentionally exclude to preserve service functionality and consumer expectations.

These definitional standards also reflect how state privacy law has evolved in recent years, including through the adoption of heightened protections for sensitive data. States such as Virginia, Colorado, and Connecticut have enacted modern privacy statutes that provide strong consumer protections while supporting consistent implementation across jurisdictions. Core elements common across those laws include:

- Opt-in consent requirements for processing sensitive data, including precise geolocation data;
- Robust consumer rights, including access, deletion, correction, and portability;
- Rights to opt out of targeted advertising, sale of personal data, and certain profiling activities;
- Risk assessment requirements for high-risk processing activities; and
- Contractual accountability requirements governing downstream data use.

Taken together, the widely adopted national privacy framework addresses sensitive data risks, including misuse of precise geolocation and other location-based data, through integrated consumer rights, controller accountability, and risk-based governance requirements that apply across data types and technologies. These laws require organizations to assess foreseeable risks, implement proportionate safeguards, and document mitigation measures before engaging in higher-risk data processing. Because these obligations apply across categories of personal data, the national model provides more durable protection against misuse of sensitive location data while remaining adaptable to evolving technologies.

SPSC recognizes Hawaii's interest in protecting residents from misuse of sensitive data. SPSC remains committed to working with the Legislature on solutions that strengthen consumer protections while maintaining alignment with widely adopted state privacy models. For these reasons, SPSC respectfully urges the Committee to oppose SB 1163 and instead consider advancing privacy legislation that provides strong protections for consumers while ensuring operational clarity and interstate interoperability.

Respectfully submitted,

Andrew A. Kingman
Counsel, State Privacy & Security Coalition