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 Commerce & Consumer Protection
Wednesday, February 25, 2026
9:45 a.m.
Via Videoconference
and
Conference Room 220

WRITTEN TESTIMONY ONLY

On the following measure:
S.B. 1163, S.D. 1, RELATING TO PRIVACY

Chair Keohokalole 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 purposes of this bill are to prohibit the sale of geolocation information and internet browser information without consent, prohibit the sale of data collected through eavesdropping or through an application operating in the background of a device that uses the device's microphone, establish exemptions for lawful investigations conducted by law enforcement agencies, customer proprietary network information, and certain telecommunication carriers.

Protecting consumers' personal data, such as geolocation and browsing history, is very important, as the unregulated sale of personal data can pose 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. We agree with the premise of this measure that stronger safeguards are needed in state law to restrict the uninhibited sale of personal data.

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. At present, we lack specialized expertise in geolocation technologies, mobile data collection, data brokers, and the technologies used and misused in privacy violations.

Many states have dedicated enforcement resources, including technologists or privacy specialists, who play a critical role in effective enforcement of measures such as this one that protect their residents' personal data. 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.

Should the committee wish to pass this bill, we respectfully request an amendment inserting a general fund appropriation of $450,000 to support the establishment of a new technologist position, a new staff attorney position, and a new investigator position, to be place within the agency designated with primary enforcement authority.

Thank you for the opportunity to testify on this bill.

STATE PRIVACY & SECURITY COALITION

February 23, 2026

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

Re: SB 1163, Senate Draft 1 – Relating to Privacy

Dear Chair Keohokalole, Vice Chair Fukunaga, 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 Senate Bill 1163, Senate Draft 1 (SB 1163). We recognize and appreciate the Committee's efforts to amend the bill and to refine its approach. However, despite those revisions, the legislation continues to present the same core structural and definitional concerns that SPSC has raised in prior testimony.

Protecting consumers from misuse of sensitive data remains a critical priority, and SPSC supports strong safeguards for information such as precise geolocation data. At the same time, 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 comprehensive state privacy statutes establish consistent consumer rights and business obligations across categories of personal data while allowing scalable and durable compliance programs. ***For that reason, and for the concerns outlined below, SPSC must respectfully oppose SB 1163, as amended.***

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.[1] The bill's 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.[2] 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

[1] *See* Covington & Burling LLP, *California Attorney General Finalizes CCPA Regulations* (June 22, 2020) (explaining that the Attorney General "refused to resolve commenters' divergent views" on how the CCPA "sale" definition should be interpreted and applied; emphasizing that whether a disclosure constitutes a "sale" requires a "fact-specific determination"; and noting the Attorney General identified open issues requiring "further study and analysis" and anticipated future clarifications), https://www.cov.com/en/news-and-insights/insights/2020/06/california-attorney-general-finalizes-ccpa-regulations#:~:text=Sales,Appendix%20A%2C%20row%2047.

[2] *See, e.g.*, Va. Code Ann. §§ 59.1-575-584 (Virginia Consumer Data Protection Act) (establishing opt-in consent for sensitive data, consumer rights, opt-out rights for targeted advertising, sale, and profiling, data protection assessments, and controller-processor contractual requirements); Colo. Rev. Stat. §§ 6-1-1301-1314 (Colorado Privacy Act) (requiring affirmative consent for sensitive data processing and imposing risk assessment and contractual accountability obligations); Conn. Gen. Stat. §§ 42-515-526 (Connecticut Data Privacy Act) (providing access, correction, deletion, and portability rights, opt-out mechanisms, and data governance standards for higher-risk processing).

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.

We appreciate the time and effort the Committee has devoted to this legislation and thank you for your consideration of our comments. Please do not hesitate to contact us with any questions or concerns.

Respectfully submitted,

Andrew A. Kingman
Counsel, State Privacy & Security Coalition

William C. Martinez
Counsel, State Privacy & Security Coalition

TECHNET
THE VOICE OF AMERICAN INNOVATION

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

February 24, 2026

Senator Jarrett Keohokalole
Chair, Committee on Commerce and Consumer Protection
Hawaii State Capitol
415 South Beretania Street, Room 229
Honolulu, HI 96813

Senator Carol Fukunaga
Vice Chair, Committee on Commerce and Consumer Protection
Hawaii State Capitol
415 South Beretania Street, Room 229
Honolulu, HI 96813

RE: SB 1163 SD1 (Lee) - Relating to Privacy - Oppose

Dear Chair Keohokalole, Vice Chair Fukunaga, and members of the committee,

On behalf of TechNet, we respectfully oppose SB 1163 SD1, which would prohibit the sale of geolocation information and internet browser information without explicit consent.

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, even as amended, the bill remains 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 narrowly tailored prohibitions on the sale of precise geolocation information. Indeed, several states restrict the sale of precise location data within comprehensive privacy statutes that include clear definitions, role distinctions, and operational exceptions.

SB 1163 SD1 instead establishes standalone prohibitions untethered from a broader privacy framework. While the bill now defines "precise location" as data locating a user within a one-mile radius, it still lacks the structural guardrails and balancing provisions found in comprehensive state privacy laws. If Hawaii seeks to regulate precise geolocation data, a comprehensive framework or targeted data broker model would provide clearer and more durable protections.

Scope Extends Well Beyond Telecommunications
The bill applies to "any person" selling covered information collected via mobile devices or location-based applications. As a result, its reach extends far beyond telecommunications providers to app developers, online platforms, advertising technology companies, data intermediaries, and cybersecurity firms.

The bill also regulates "internet browser information," which includes browsing history, application usage history, IP origin and destination addresses, device identifiers, and even the content of communications that make up internet activity. This covers a broad range of data that extends well beyond the stated focus on geolocation privacy.

Overbreadth and Ambiguity in Additional Data Categories
The bill prohibits the sale of data collected through "eavesdropping" and through background applications using a device's microphone, yet these terms remain undefined. It is unclear what constitutes "eavesdropping" data, what specific categories of information are covered, or whether the prohibition extends beyond audio content to unrelated technical signals.

This lack of precision introduces significant compliance risk and regulatory uncertainty.

Unintended Consequences for Cybersecurity and Fraud Prevention
SB 1163 SD1 contains no exemption for legitimate cybersecurity or fraud prevention activities. In practice, geolocation signals, IP addresses, and device identifiers are essential tools for detecting anomalous behavior, preventing account takeovers, and responding to threats in real time.

By broadly restricting the sale of these signals without operational carveouts, the bill risks weakening security infrastructure. It would effectively require malicious actors to consent to the sharing of information used to detect them—an outcome that undermines consumer protection and public safety.

Protecting sensitive location information is an important policy goal. However, SB 1163 SD1 continues to adopt a fragmented and overbroad approach that extends beyond its stated intent, lacks necessary definitions and operational exceptions, and risks disrupting legitimate data uses.

TECHNET
THE VOICE OF AMERICAN INNOVATION

For these reasons, we respectfully oppose the bill and urge the Legislature to pursue a more coherent, evidence-based privacy framework for 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

February 24, 2026

Senator Jarrett Keohokalole
Chair, Senate Committee on Commerce and Consumer Protection
Hawaii State Capitol, Room 205
Honolulu, HI 96813

Senator Carol Fukunaga
Vice Chair, Senate Committee on Commerce and Consumer Protection
Hawaii State Capitol, Room 216
Honolulu, HI 96813

RE: Letter in Opposition to Hawaii SB 1163

Dear Chair Keohokalole and Vice Chair Fukunaga:

On behalf of the advertising industry, we write to oppose Hawaii SB 1163, as amended by SD 1.[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 Commerce and Consumer Protection ("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

---

[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.

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 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.

---

[5] SB 1163 § 2.

[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.

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 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 Senate Committee on Commerce and Consumer Protection

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

LATE

Testimony of
JAKE LESTOCK
CTIA

In Opposition to Hawaii Senate Bill 1163

Before the
Senate Committee on Commerce and Consumer Protection

February 24, 2026

Chair Keohokalole, Vice Chair Fukunaga, and members of the committee, on behalf of CTIA®, the trade association for the wireless communications industry, I submit this testimony in opposition to Senate Bill 1163. CTIA and our members support strong consumer privacy protections that empower consumers and enhance privacy and security, while still allowing for innovative and beneficial uses of data, including location data -- particularly uses that consumers expect and that are necessary to provide, maintain, and secure communications services. We agree with the goal of protecting consumers from the misuse of sensitive location data and internet browsing information. However, as drafted, SB 1163 is both overbroad and underinclusive in ways that could (1) disrupt routine, pro-consumer operational practices, (2) create loopholes that leave consumers unprotected, and (3) increase confusion and complexity without delivering comprehensive privacy benefits.

Rather than adopting a narrow, carve-out bill that departs from the direction of modern state privacy frameworks, we urge the Legislature to abandon this approach and

instead pursue a comprehensive, interoperable privacy law that provides consistent protections across the data ecosystem.

I. SB 1163 is overbroad: it risks disrupting routine, non-sale information sharing that consumers expect

SB 1163 broadly regulates the "sale" of sensitive location data and internet browsing information. CTIA is concerned that the bill's definition of "sale" does not sufficiently account for routine disclosures that are not sales and are necessary to deliver services consumers request and rely on every day.

In modern networks and digital services, companies must share limited data with vendors and service providers to:

- **Provide requested services** (e.g., deliver connectivity, support an app's core functions, complete transactions)
- **Maintain and repair networks** (including outage response, performance monitoring, and troubleshooting)
- **Improve networks and services** (quality of service, capacity planning, and reliability enhancements)
- **Detect and prevent fraud** (account takeovers, identity fraud, SIM swap and similar threats)
- **Protect security** (incident response, vulnerability detection, abuse prevention, and compliance monitoring)

If “sale” is defined so broadly that these routine, operational disclosures are treated like commercial data brokerage, SB 1163 could inadvertently require opt-in consent for core practices that are essential to privacy and security, not opposed to them.

Practical example: fraud prevention and account security

Fraud detection often relies on signals that can include device location indicators. If a provider sees a login attempt from Hawaii while a trusted device signal indicates the consumer is elsewhere, that can be a strong indicator of account takeover. Conversely, matching signals may help confirm legitimate travel. A framework that inadvertently restricts routine security and fraud uses—by treating necessary disclosures as a “sale”—could weaken protections for consumers.

Bottom line: Consumers benefit when privacy laws target harmful conduct without interfering with ordinary, pro-consumer operations like service provisioning, fraud prevention, and security.

II. SB 1163 is underinclusive: it applies to only a narrow subset of companies, leaving consumers exposed elsewhere

SB 1163 appears to apply only to a limited set of entities in the data ecosystem. That design creates a major policy gap: the same sensitive data may remain unprotected when collected, used, or shared by others outside the bill’s scope.

This is problematic for three reasons:

1. It fails to comprehensively protect consumers. Consumers do not experience privacy risk in "silos." They expect protections to follow the data, not the type of company holding it.
2. It distorts competition. Targeting only some participants can create uneven compliance burdens that advantage non-covered entities—even when they collect the same categories of sensitive data.
3. It increases consumer confusion. If protections vary depending on who collects the information rather than what the information is and how it's used, consumers cannot easily understand their rights or make informed choices.

If the Legislature's objective is to protect sensitive location and browsing information, the policy should address those data consistently across the market, not solely for a narrow subset of companies.

III. SB 1163 defines "geolocation information" more broadly than other state privacy laws, expanding "sensitive" beyond precision and accuracy

Modern state privacy laws generally treat precise geolocation data as sensitive, with an opt-in consent model for certain processing. Importantly, those laws typically define "precise geolocation" with a focus on accuracy and precision (e.g., identifying a person's location within a small radius), not a sweeping concept that could capture generalized location indicators.

SB 1163's definition of "geolocation information" is so broad that it risks capturing information that is not meaningfully "precise" or sensitive in the way consumers and lawmakers typically intend—potentially including generalized location indicators such as a ZIP code or other coarse location data. That expansion can create compliance obligations that are mismatched to actual risk, while also undermining clarity and interoperability with other state laws.

A more workable approach—consistent with the prevailing model in other states—is to focus on appropriately defined precise geolocation data, rather than redefining "location" so broadly that routine, low-risk data becomes regulated as if it were GPS-level precision.

IV. The bill's approach departs from the direction of comprehensive state privacy frameworks

To date, twenty states have enacted comprehensive consumer privacy laws. While details vary, the dominant approach in these frameworks includes:

- Treating precisely defined precise geolocation data as sensitive data, commonly subject to heightened protections (often opt-in consent for processing).
- Providing opt-out rights for the sale of personal data, typically with reasonable exceptions to ensure routine business operations and service-provider relationships can function.
- Requiring opt-in consent for processing sensitive data and/or for secondary, unexpected uses that consumers would not reasonably anticipate.

- Ensuring that routine and necessary business operations, like network repair and improvement, fraud detection, and security are allowed, subject to reasonable data minimization requirements.

By contrast, SB 1163 attempts to address discrete data types with unusually broad definitions and consent requirements while applying only to a narrow segment of the ecosystem. That combination increases fragmentation, operational risk, and consumer confusion—without achieving comprehensive coverage.

V. Existing federal and state authorities already address key harms, and CTIA continues to support a uniform national standard

CTIA supports strong privacy protections and recognizes that multiple legal authorities already address harmful or deceptive practices involving sensitive data.

- The Federal Trade Commission (FTC) has long treated precise geolocation as sensitive in its privacy guidance and has brought enforcement actions where companies misrepresented consumer control or engaged in unfair or deceptive practices.
- As the amended version of SB 1163 recognizes, the Federal Communications Commission (FCC) regulates carriers' use of Customer Proprietary Network Information (CPNI), which can include certain location-related information depending on context.
- The Hawaii Attorney General has authority under Hawaii's consumer protection laws to address unfair or deceptive acts and practices.

These existing authorities reduce the need for Hawaii to adopt an overbroad, ecosystem-fragmenting approach—particularly one that risks disrupting legitimate security, fraud, and service-delivery practices.

CTIA continues to prefer a national privacy standard to ensure consistent protections for consumers and predictable compliance obligations for businesses operating across state lines. However, regardless of federal action, if Hawaii is poised to legislate, the most durable path is a comprehensive privacy framework that applies evenly across covered entities and data types.

VI. Conclusion

CTIA supports strong consumer privacy protections, including safeguards for sensitive location and browsing information. But SB 1163, as drafted, is overbroad in ways that could interfere with routine service, security, and fraud-prevention practices—and underinclusive in ways that leave consumers exposed and distort competition.

For these reasons, CTIA respectfully urges the legislature to reject broadly drafted legislation like this bill that could have serious operational impacts and hinder innovation and security. Comprehensive legislation setting forth clear and interoperable standards is the only way to ensure clear, consistent privacy protection for consumers and certainty for businesses. For these reasons, CTIA respectfully requests that you do not move this legislation.

LATE

SB-1163-SD-1
Submitted on: 2/24/2026 1:42:44 PM
Testimony for CPN on 2/25/2026 9:45:00 AM

Submitted By	Organization	Testifier Position	Testify
Jen Wilbur	Testifying for Planned Parenthood Alliance Advocates	Support	Written Testimony Only

Comments:

Planned Parenthood Alliance Advocates supports SB 1163, which would add much needed data privacy regulation, and asks that this measure be voted out favorably by the Senate Committee on Consumer Protection and Commerce.

LATE

Hawaiian Telcom

Written Statement of

Jeannine Souki,
Senior Manager – Government & Regulatory Affairs

SENATE COMMITTEE ON COMMERCE & CONSUMER PROTECTION
February 25, 2026, 9:45 AM
State Capitol, Conference Room 229 & Videoconference

COMMENTS AND REQUEST TO AMEND:

SB 1163, S.D. 1 – RELATING TO PRIVACY

To: Chair Keohokalole, Vice Chair Fukunaga, and Members of the Committee
Re: Testimony providing comments for SB1163, SD 1

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

My name is Jeannine Souki, Senior Manager of Government & Regulatory Affairs at Hawaiian Telcom. Mahalo for the opportunity to provide **comments on SB1163, SD1 Relating to Privacy**.

SB1163, SD1 seeks to strengthen consumer privacy by prohibiting the sale of sensitive geolocation and internet browser information, as well as data collected through eavesdropping or background applications, without consent. Hawaiian Telcom supports these goals to enhance customer protections.

We appreciate that SD1 now includes important exemptions for:

- **Customer Proprietary Network Information (CPNI)**, and
- **Telecommunications carriers acting in compliance with federal CPNI requirements**

These updates ensure the bill aligns with federal telecommunications privacy law under **47 U.S.C. § 222**, which already imposes strict rules on how carriers use, disclose, and safeguard CPNI, with federal regulations further defining and enforcing these obligations.

By incorporating these exemptions, SB1163, SD1 avoids duplicative or conflicting regulatory requirements while maintaining protections for consumers—particularly regarding the sale of sensitive, non-telecommunications geolocation data. Hawaiian Telcom supports this balanced approach, which appropriately recognizes existing federal requirements while advancing privacy protections for Hawai‘i residents.

Mahalo for the opportunity to provide comments on SB1163, SD1.

SB-1163-SD-1
Submitted on: 2/20/2026 7:12:26 PM
Testimony for CPN on 2/25/2026 9:45:00 AM

Submitted By	Organization	Testifier Position	Testify
Lorna Holmes	Individual	Support	Written Testimony Only

Comments:

I urge you to pass this bill to protect the citizens of Hawaii from having our private information monetized without permission. Due to the excessive influence of tech corporate interests on the federal government, we cannot expect the neccessary regulation to come from that source, and must rely on the State.

Mahalo for your consideration,

Dr. Lorna Holmes, Mo'il'ili 96826