



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

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

SYLVIA LUKE
LIEUTENANT GOVERNOR | KA HOPE KIA'ĀINA

NADINE Y. ANDO
DIRECTOR | KA LUNA HO'OKELE

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

Testimony of the Department of Commerce and Consumer Affairs

**Before the
House Committee on Consumer Protection & Commerce
Tuesday, February 10, 2026
2:00 p.m.
Via Videoconference
Conference Room 329**

**On the following measure:
H.B. 1753, RELATING TO SOCIAL MEDIA**

Chair Matayoshi and Members of the Committee:

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

H.B. 1753 gives Hawaii residents the right to remove their presence online when they close a social media account. Currently, many social media companies intentionally make it hard to leave their platforms, using confusing menus or "dark patterns" to keep users and their data locked in. This bill fixes that by requiring a simple, one-click style deletion process. More importantly, it ensures that "deletion" actually means the data is gone—not just hidden or archived—which protects consumers from future data breaches and identity theft.

We support the provision that prevents companies from demanding extra personal information just to process a deletion. The bill could provide added protections by adopting the more detailed definitions found in the California Consumer Privacy Act (CCPA). Specifically, Hawaii should follow California's lead in classifying "Unique Identifiers" and "Inferences" as personal information.

California's definition of "personal information" includes "invisible" data like tracking cookies, IP addresses, and digital beacons. Without these specific provisions, a company could delete your account but still track your device using a "unique identifier" loophole.

California also protects "Inferences"—the hidden profiles companies build to guess your habits, health, or religion. Adopting language similar to the CCPA's definition of personal information and sensitive personal information would ensure that a deletion request wipes out a user's entire "digital twin," preventing tech companies from holding onto private details under the excuse that the data is "anonymous."

Should the Committee wish to pass this bill, we respectfully request:

(1) replacing the definition of "personal information" beginning on Page 2, Line 20, with the following definition:

"Personal information" means 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. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

Testimony of DCCA

H.B. 1753

Page 3 of 5

(B) Any personal information described in section 487N-1.

(C) Characteristics of protected classifications under Hawaii or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(L) Sensitive personal information.

"Personal information" does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. "Publicly available" means any of the following:

Testimony of DCCA

H.B. 1753

Page 4 of 5

(I) Information that is lawfully made available from federal, state, or local government records.

(II) Information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media.

(III) Information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.

"Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. **(2) Adding the following definition of "sensitive personal**

information":

Sensitive personal information" means:

(A) Personal information that reveals:

(i) A consumer's social security, driver's license, state identification card, or passport number.

(ii) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

(iii) A consumer's precise geolocation.

(iv) A consumer's racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.

(v) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.

(vi) A consumer's genetic data; or

(vii) A consumer's neural data.

"Neural data" means information that is generated by measuring the activity of a consumer's central or peripheral

Testimony of DCCA

H.B. 1753

Page 5 of 5

nervous system, and that is not inferred from nonneural information.

(B) The processing of biometric information for the purpose of uniquely identifying a consumer;

(C) Personal information collected and analyzed concerning a consumer's health; and

(D) Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

(3) Adding the phrase "and sensitive personal information" after the phrase "personal information" at Page 2, Line 16, Page 2, Line 18, Page 3, Line 14, Page 3, Line 18, Page 4, Line 2, Page 4, Line 4, Page 4, Line 9,

Thank you for the opportunity to testify on this bill.

February 9, 2026

Representative Scot Z. Matayoshi
Chair, Committee on Consumer Protection & Commerce
Hawaii State Capitol
415 South Beretania Street, Room 329
Honolulu, HI 96813

RE: HB 1753 (Templo) – Social Media Account Deletion - Concerns

Dear Chair Matayoshi, and members of the committee,

On behalf of TechNet, we write to express concerns regarding HB 1753, the Hawaii Social Media Data Deletion Act.

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 support the goal of providing users with meaningful control over their personal information and appreciate the Legislature's focus on data deletion transparency. However, as drafted, the bill includes several provisions that would create uncertainty, impose infeasible obligations, and diverge from established privacy frameworks.

Definition of "Delete" Requires Technical Feasibility Recognition

HB 1753 defines "delete" to suggest the complete and immediate removal of personal information from all systems. Most privacy laws rely on the ordinary meaning of deletion and recognize that complete removal may not always be technically feasible, particularly with respect to archived or backup systems. We recommend clarifying that deletion should be required to the extent technically feasible and as otherwise permitted by state or federal law, consistent with consensus privacy frameworks.

Definition of "Personal Information."

The bill's definition of "personal information" should be aligned with widely adopted U.S. privacy laws that define the term as information that is linked or reasonably

linkable to an identified or identifiable individual. Alignment would provide clarity and reduce interpretive uncertainty for covered platforms.

Lack of a Definition for “User” Raises Extraterritorial Concerns

HB 1753 does not define the term “user,” which could be interpreted to include any person located in Hawaii, regardless of residency or context. We recommend adding a definition consistent with the consensus definition of “consumer” in U.S. privacy laws—limited to Hawaii residents acting in an individual or household context—to avoid unintended extraterritorial application.

Clarification of Account Deletion Obligations

Section 2(b) raises several operational concerns. First, requiring deletion of all personal information “associated with” an account introduces significant ambiguity compared to the more common standard of data “provided by” the user. Second, the use of the term “erase” conflicts with the bill’s defined term “delete.” Third, the timing and notification requirements could be read to require immediate deletion or post-deletion notice after an account no longer exists, which would be infeasible.

Targeted revisions clarifying scope, terminology, and sequencing would make this provision workable while preserving the bill’s intent.

Deletion Timelines, Recordkeeping, and Rulemaking Provisions Create Uncertainty

While HB 1753 requires deletion within forty-five days, it does not account for situations where deletion across complex systems cannot be completed within that timeframe. We recommend allowing a one-time forty-five-day extension when reasonably necessary, consistent with other privacy laws, and permitting a short delay to allow users to rescind deletion requests.

The bill also requires platforms to maintain records of deletion requests for an unspecified number of years, creating uncertainty and compliance risk. In addition, broad rulemaking authority for the Attorney General may be unnecessary if statutory clarity is achieved through the targeted amendments described above.

Definition of “Social Media Platform” Concerns

Lastly, we are concerned that the definition of “social media platform” is drafted so broadly that it could encompass services not commonly understood to be social media platforms. This lack of precision risks sweeping in unrelated services and warrants further refinement.

HB 1753 raises important issues regarding user control over personal information, but several provisions would benefit from clarification and alignment with established privacy standards. We respectfully urge the Committee to consider targeted amendments to address these concerns and ensure the bill is workable, precise, and effective.

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

Sincerely,

A handwritten signature in blue ink, appearing to read "Robert Boykin".

Robert Boykin
Executive Director for California and the Southwest
TechNet

LATE

HB-1753

Submitted on: 2/9/2026 10:20:29 PM

Testimony for CPC on 2/10/2026 2:00:00 PM

Submitted By	Organization	Testifier Position	Testify
Christian Kaakua	Individual	Support	Written Testimony Only

Comments:

Aloha Chair Matayoshi, Vice Chair Grandinetti, and Members of the House Committee on Consumer Protection & Commerce,

My name is Christian, and I am a high school student from Oahu, testifying in support of HB1753, advocating that social media platforms should be required to make the erasure of personal information easy and accessible.

As a keiki growing up in the Digital Age, I can clearly see the widespread effects social media has had on my classmates, friends, and generation as a whole. I think everyone, but especially kids who have a social media presence, should have the unequivocal right to pull back from social media completely. Passing this bill also supports our right to privacy.

For these reasons, I believe this bill, HB1753, should be passed.

Thank you for your consideration.