HOUSE OF REPRESENTATIVES
THIRTY-THIRD LEGISLATURE, 2026
STATE OF HAWAII

H.B. NO. 2463

A BILL FOR AN ACT

RELATING TO CONSUMER PRIVACY.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

SECTION 1. The legislature finds that the right to privacy is a fundamental right guaranteed to the people of the State of Hawaii by the Hawaii State Constitution. This right reflects the deeply held values of the people of Hawaii. Furthermore, the Hawaii State Constitution imposes upon the legislature an affirmative duty to safeguard the personal privacy, dignity, and security of Hawaii's residents.

The legislature further finds that, in the modern digital economy, this constitutional right to privacy is increasingly undermined by the widespread and largely invisible practices of the data brokerage industry. Thousands of companies operate in an intentionally opaque marketplace, quietly collecting, aggregating, analyzing, and selling vast quantities of personal information about individuals— often without their knowledge, awareness, or meaningful consent. These practices occur outside of any direct relationship between the individual and the entity profiting from their personal data.

Residents of Hawaii routinely have their names, home addresses, phone numbers, geolocation histories, purchasing habits, family relationships, and behavioral profiles collected and sold to third parties they have never heard of and cannot reasonably identify or contact. This ecosystem is deliberately fragmented and difficult to navigate, making it effectively impossible for consumers to understand who is collecting their data, how it is being used, or to exercise meaningful control over its dissemination.

The legislature finds that this lack of transparency and accountability poses a serious risk not only to personal privacy, but also to public safety. Data collected and sold by brokers may be exploited by bad actors for stalking, harassment, identity theft, fraud, intimidation, and other nefarious purposes. Victims of domestic violence, stalking survivors, seniors, and other vulnerable populations are particularly at risk when sensitive personal information is freely traded without their knowledge or consent.

Therefore, residents of Hawaii must have a clear and enforceable right to know which entities are collecting and selling their personal information, and a meaningful ability to

opt out of such collection and sale. Privacy rights that exist only on paper, or that require consumers to navigate a maze of hidden actors and inconsistent processes, do not satisfy the constitutional promise of privacy.

Accordingly, the purpose of this Act is to:

(1) Require data brokers to register annually with the Department of Commerce and Consumer Affairs;

(2) Establish an accessible deletion mechanism of personal data;

(3) Establish penalties for non-compliance;

(4) Establish a private right of action; and

(5) Establish a Consumer Privacy Fund.

SECTION 2. The Hawaii Revised Statutes is amended by adding a new chapter to be appropriately designated and to read as follows:

"CHAPTER

HAWAII DROP AND DELETE ACT

PART I. GENERAL PROVISIONS

§ -1 Definitions. As used in this chapter:

"Aggregate consumer information" means information that relates to a group or category of consumers, from which

individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not include one or more individual consumer records that have been deidentified.

"Biometric information" means an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid, which can be used singly or in combination with each other or with other identifying data to establish individual identity. "Biometric information" includes imagery of the iris, retina, fingerprint, face, hand, palm, or vein patterns; voice recordings from which an identifier template, such as a faceprint, minutiae template, or voiceprint, can be extracted; and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

"Business" has the same meaning as in section 487J-1.

"Collect", "collected", or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means,

including receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

"Consumer" means an individual residing in the State.

"Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the personal information of a consumer with whom the business does not have a direct relationship. "Data broker" does not include:

(1) An entity to the extent that it is covered by the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(2) An entity to the extent that it is covered by the Gramm-Leach-Bliley Act, P.L. 106-102, and implementing regulations; or

(3) An entity to the extent that it is covered by chapter 431, article 3A.

"Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.

"Device" means any physical object that is capable of connecting to the internet, directly or indirectly, or to another device.

"Direct relationship" means a relationship, past or present, between a consumer and a business in which the consumer knowingly and intentionally engages with the business for the primary purpose of obtaining goods or services from that business, and in which the business collects personal information directly from the consumer in the course of that interaction. "Direct Relationship" includes circumstances in which the consumer is a customer, client, subscriber, or user of the business's goods or services; an employee, contractor, or agent of the business; an investor in the business, or a donor to the business. "Direct Relationship" does not include:

(1) The passive collection of personal information through tracking technologies, including cookies pixels, beacons, software development kits, device fingerprinting, or similar technologies;

(2) The collection, purchase, licensing, or receipt of personal information from a third party, data broker, or affiliate, regardless of whether the consumer

interacted with a website, application, or service that enabled such collection;

(3) A relationship created solely by a consumer's use of a device, application, website, or service where the primary purpose of the interaction is to enable advertising, analytics, profiling, or data monetization rather than the provision of goods or services requested by the consumer;

(4) A relationship inferred or constructed based on a consumer's presence, behavior, or activity, including browsing, location, or application usage, without an affirmative act by the consumer directed towards establishing a relationship with the business;

(5) The collection of personal information incidental to providing infrastructure, background services, or third-party support services, including cloud services, content delivery networks, payment processing, or advertising services; or

(6) Any relationship established through consent obtained via pre-checked boxes, bundled consent, dark patterns, or terms of service that do not provide a clear and

meaningful choice regarding the collection or sale of personal information.

"Family" means any group of individuals related to a consumer by blood, marriage, domestic partnership, civil union, adoption, guardianship, custody, or other legally recognized familial relationship.

"License" means to grant one's business access to, or distribution of, data to another business in exchange for consideration. "License" does not include the sharing of data for the sole benefit of the business providing the data, where that business maintains sole control over the use of the data.

"Office" means the office of consumer protection.

"Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, or any other organization or group of persons acting in concert.

"Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes the following:

(1) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier internet protocol address, electronic mail address, account name, social security number, driver's license number, passport number, or other similar identifiers;

(2) Personal information as defined in section 487N-1;

(3) Characteristics of protected classifications under federal or state law;

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

(5) Biometric information;

(6) Internet or other electronic network activity information, including browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement;

(7) Geolocation information;

(8) Audio, electronic, visual, thermal, olfactory, or similar information;

(9) Professional or employment-related information;

(10) 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. 1232g; 34 C.F.R. part 99); and

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

"Publicly available" means available information from federal, state, or local government records, including any conditions associated with the information. "Publicly available" does not include:

(1) Biometric information collected by a business about a consumer without the consumer's knowledge; and

(2) Consumer information that is deidentified or aggregate consumer information.

"Sell", "selling", "sale", or "sold" means selling, 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 another business or a third party for monetary or other valuable consideration.

"Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, family, or device that is linked to a consumer or family, over time and across different services, including but not limited to a device identifier; an internet protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device.

"Verifiable consumer request" means a request made by a consumer, or on behalf of the consumer's minor child, whom the business verifies is a consumer of the business's services.

PART II. DATA BROKERS

§ -2 **Annual registration.** (a) On or before January 31 of each year following a year in which a business meets the definition of data broker, a data broker shall:

(1) Register with the office;

(2) Pay a registration fee in an amount determined by the office, to be deposited into the consumer privacy special fund; and

(3) Provide the following information to the office:

(A) The name and primary physical, electronic mail, and internet addresses of the data broker;

(B) If the data broker permits a consumer to opt out of the data broker's collection of personal information, opt out of its databases, or opt out of certain sales of data:

(i) The method for requesting an opt-out;

(ii) Which activities and sales the opt-out applies to; and

(iii) Whether the data broker permits a consumer to authorize a third party to perform the opt-out on the consumer's behalf;

(C) A statement specifying the data collection, databases, or sales activities from which a consumer may not opt out; and

(D) Any additional information or explanation the data broker chooses to provide concerning its data collection practices.

(b) The office shall create a page on its website where the information provided by data brokers under this chapter shall be accessible to the public.

(c) A data broker that fails to register with the office as required by this section shall be liable for administrative fines and costs in an administrative action brought by the office as follows:

(1) An administrative fine as determined by the office for each day the data broker fails to register as required by this section;

(2) An amount equal to the fees that were due during the period it failed to register; and

(3) Expenses incurred by the office in the investigation and administration of the action as the court deems appropriate.

(d) Any penalties, fines, fees, and expenses received pursuant to subsection (c) shall be deposited in the consumer privacy fund.

§ -3 **Personal information; deletion.** (a) The office shall establish an accessible deletion mechanism that:

(1) Implements and maintains reasonable security procedures and practices, including but not limited to administrative, physical, and technical safeguards appropriate to the nature of the information and the purposes for which the personal information will be used and to protect consumers' personal information from unauthorized use, disclosure, access, destruction, or modification;

(2) Allows a consumer, through a single verifiable consumer request, to request that every data broker that maintains any personal information delete any personal information related to that consumer held by the data broker or associated service provider or contractor;

(3) Allows a consumer to selectively exclude specific data brokers from a request made under paragraph (2); and

(4) Allows a consumer to make a request to alter a previous request made under this subsection after at least forty-five days have passed since the consumer last made a request under this subsection.

(b) The accessible deletion mechanism established pursuant to subsection (a) shall meet the following requirements:

(1) The accessible deletion mechanism shall allow a consumer to request the deletion of all personal information related to that consumer through a single deletion request;

(2) The accessible deletion mechanism shall permit a consumer to securely submit information in one or more privacy-protecting ways determined by the office to aid in the deletion request;

(3) The accessible deletion mechanism shall allow data brokers registered with the office to determine whether an individual has submitted a verifiable consumer request to delete the personal information related to that consumer as described in paragraph (1) and shall not allow the disclosure of any additional personal information when the data broker accesses the

accessible deletion mechanism, unless otherwise specified in this chapter;

(4) The accessible deletion mechanism shall allow a consumer to make a request described in paragraph (1) using an internet service operated by the office;

(5) The accessible deletion mechanism shall not charge a consumer to make a request as described in paragraph (1);

(6) The accessible deletion mechanism shall allow a consumer to make a request as described in paragraph (1) in any language spoken by any consumer for whom personal information has been collected by data brokers;

(7) The accessible deletion mechanism shall be readily accessible and usable by consumers with disabilities;

(8) The accessible deletion mechanism shall support the ability of a consumer's authorized agents to aid in the deletion request;

(9) The accessible deletion mechanism shall allow the consumer, or the consumer's authorized agent, to

verify the status of the consumer's deletion request; and

(10) The accessible deletion mechanism shall provide a description of all of the following:

(A) The deletion permitted by this section, including but not limited to the actions required by subsections (c), (d), and (e);

(B) The process for submitting a deletion request pursuant to this section; and

(C) Examples of the types of information that may be deleted.

(c) A data broker shall access the accessible deletion mechanism established pursuant to subsection (a) at least once every forty-five days and shall conduct the following:

(1) Within forty-five days after receiving a request made pursuant to this section, process all deletion requests made pursuant to this section and delete all personal information related to the consumers making the requests consistent with the requirements of this section;

(2) In cases where a data broker denies a consumer request to delete under this chapter because the request cannot be verified, process the request and refrain from selling or sharing the consumer's personal information or using or disclosing the consumer's sensitive personal information; provided that the data broker shall request, after at least twelve months after processing the consumer request, the consumer to authorize the sale or sharing of the consumer's personal information or the use and disclosure of the consumer's sensitive personal information;

(3) Direct all service providers or contractors associated with the data broker to delete all personal information in their possession related to the consumers making the requests described in paragraph (1); and

(4) Direct all service providers or contractors associated with the data broker to process a request described by paragraph (2) as an opt-out of the sale or sharing of the consumer's personal information.

(d) A data broker shall delete all personal information of a consumer at least once every forty-five days pursuant to this section after the consumer has submitted a deletion request and a data broker has deleted the consumer's data pursuant to this section unless the consumer requests otherwise or the deletion is not required pursuant to subsection (f).

(e) A data broker shall not sell or share new personal information of the consumer after a consumer has submitted a deletion request and a data broker has deleted the consumer's data pursuant to this section unless the consumer requests otherwise or selling or sharing the personal information is permitted under subsection (d).

(f) Notwithstanding subsection (c), a data broker shall not be required to delete a consumer's personal information if either of the following apply:

(1) It is reasonably necessary for the data broker to maintain the personal information to:

(A) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or

service requested by the consumer, or reasonably anticipated by the consumer within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer;

(B) Help to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes;

(C) Debug to identify and repair errors that impair existing intended functionality;

(D) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law;

(E) Engage in public or peer-reviewed scientific, historical, or statistical research that conforms or adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the ability to complete such

research, if the consumer has provided informed consent;

(F) Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business and compatible with the context in which the consumer provided the information; or

(G) Comply with a legal obligation; or

(2) The deletion is not required to:

(A) Comply with federal, state, or county laws or comply with a court order or subpoena to provide information;

(B) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or county authorities;

(C) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or county law;

(D) Cooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury; provided that:

(i) The request is approved by the head of the entity for emergency access to a consumer's personal information;

(ii) The request is based on the agency's good faith determination that it has a lawful basis to access the information on a nonemergency basis; and

(iii) The agency agrees to petition a court for an appropriate order within three days and to destroy the information if that order is not granted;

(E) Exercise or defend legal claims;

(F) Collect, use, retain, sell, share, or disclose consumers' personal information that is deidentified or aggregate consumer information;

(G) Collect, sell, or share a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of the State; or

(H) Comply with any federal or state law protecting medical or health information.

(g) Personal information described in subsection (f) shall only be used for the purposes described in subsection (f) and shall not be used or disclosed for any other purpose, including but not limited to marketing purposes.

(h) Beginning January 1, 2027, and every three years thereafter, a data broker shall undergo an audit by an independent third party to determine compliance with this section. The data broker shall submit a report resulting from the audit and any related materials to the office within five business days of a written request from the office. A data broker shall maintain the report and materials for at least six years following completion of the audit.

(i) A data broker required to register under this chapter that fails to comply with the requirements of this section shall

be liable for administrative fines and costs in an administrative action brought by the office as follows:

(1) An administrative fine as determined by the office for each deletion request for each day the data broker fails to delete information pursuant to this section; and

(2) Reasonable expenses incurred by the office in the investigation and administration of the action.

(j) Any penalties, fines, fees, and expenses received pursuant to subsection (i) shall be deposited in the consumer privacy special fund.

§ -4 **Consumer privacy fund.** (a) There is established in the state treasury the consumer privacy fund, into which shall be deposited:

(1) Registration fees collected pursuant to section -2(a)(2);

(2) Any penalties, fines, fees, and expenses received pursuant to sections -2(d) and -3(j);

(3) Appropriations made by the legislature for deposit into the special fund;

(4) Any grant or donation made to the special fund; and

(5) Any interest earned on the balance of the special fund.

(b) Moneys in the special fund shall be expended for:

(1) The costs of establishing and maintaining the informational website described in section -2(b);

(2) The costs incurred by the state courts and the office in connection with enforcing this chapter; and

(3) The costs of establishing, maintaining, and providing access to the accessible deletion mechanism described in section -3(a).

§ -5 **Rules.** The office shall adopt rules pursuant to chapter 91 necessary to effectuate this chapter.

§ -6 **Limitation of administrative action.** No administrative action brought pursuant to this chapter alleging a violation of any of the provisions of this chapter shall commence more than five years after the date on which the violation occurred.

§ -7 **Private Right of Action.** (a) Any consumer whose personal information is collected, sold, licensed, shared, retained, or not deleted by a data broker in violation of this chapter may bring a civil action against the data broker.

(b) A consumer may bring an action under this section only if:

(1) The consumer has submitted a verifiable consumer request pursuant to section -3; and

(2) The data broker failed to comply with the requirements of this chapter within the time periods described.

(c) In an action brought under this section, a court may award:

(1) Actual damages suffered by the consumer as a result of the violation or statutory damages of not less than $300 and not more than $1000 per violation;

(2) Injunctive or declaratory relief, including an order requiring deletion of personal information or prohibiting further sale or sharing; and

(3) Reasonable attorney's fees and costs.

(d) A data broker shall not be liable for statutory damages under this section if the data broker cured the violation within thirty days after receiving written notice from the consumer describing the specific violation.

(e) Nothing in this section shall be constructed to:

(1) Limit the authority of the office to bring an administrative or enforcement under this chapter; or

(2) Preclude any consumer from pursuing any other remedy available under state or federal law.

(f) An action under this section shall be commenced within four years after the date the consumer knew or reasonably should have known of the violation.

(g) Each action to delete personal information relating to a consumer following a verifiable consumer request shall constitute a separate violation."

SECTION 3. This Act shall take effect upon its approval.

INTRODUCED BY: _____

JAN 27 2026

H.B. NO. 2463

Report Title:
Consumer Protection; Consumer Privacy; Data Brokers; Registration; Consumer Privacy Fund; Special Fund

Description:
Establishes the Hawaii Drop and Delete Act to limit the information data brokers collect and sell regarding consumer information. Establishes a deletion mechanism allowing consumers to request data brokers to drop their personal information. Establishes the consumer privacy fund. Establishes a private right of action.

The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.