HOUSE OF REPRESENTATIVES
THIRTIETH LEGISLATURE, 2020
STATE OF HAWAII

H.B. NO. 2572 H.D. 1

A BILL FOR AN ACT

RELATING TO PRIVACY.

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

PART I

SECTION 1. The legislature finds that House Concurrent Resolution No. 225, Senate Draft 1 (2019), established the twenty-first century privacy law task force, whose membership consisted of individuals in government and the private sector with an interest or expertise in privacy law in the digital era. The resolution found that public use of the internet and related technologies has significantly expanded in recent years, and that a lack of meaningful government regulation has resulted in personal privacy being compromised. Accordingly, the legislature requested that the task force examine and make recommendations regarding existing privacy laws and regulations to protect the privacy interests of the people of Hawaii.

The legislature further finds that the task force considered a spectrum of related privacy issues which have been raised in Hawaii and other states in recent years. Numerous states have begun to address the heightened and unique privacy

risks that threaten individuals in the digital era of the twenty-first century. Dozens of states have already adopted components of privacy law contained in this Act. California has enacted a comprehensive privacy act, and states such as Minnesota, New York, Virginia, and Washington are considering comprehensive legislation during their current legislative sessions.

The legislature finds that, following significant inquiry and discussion, the task force made the following seven recommendations.

First, the task force recommended that the definition of "personal information" in chapter 487N, Hawaii Revised Statutes, should be updated and expanded, as the current definition of "personal information" is outdated and needs to be amended. Individuals face too many identifying data elements that, when exposed to the public in a data breach, place an individual at risk of identity theft or may compromise the individual's personal safety. Chapter 487N, which requires the public to be notified of data breaches, is not, it its current form, comprehensive enough to cover the additional identifiers. Accordingly, that chapter's definition of "personal information"

should be updated and expanded to include various personal identifiers and data elements that are found in more comprehensive laws.

Second, the task force recommended that explicit consent be required before an individual's identifying data may be used, shared, or sold, and individuals should have the right to know what data relates to them, the ability to opt in or out of its use, and the right to delete it. An individual's identifying data can be used, sold, and purchased without consent, and many people do not know that they are susceptible to this risk.

Third, the task force recommended that explicit consent be required before an individual's geolocation data may be shared or sold to a third party. Numerous reports have been raised in which a person's real time location is identified, allowing the person to be tracked without that person's knowledge or consent by third parties, who in turn share or sell the real time location. This scenario creates serious privacy and safety concerns.

Fourth, the task force recommended that explicit consent be required before an individual's internet browser history and content accessed may be shared or sold to a third party.

Fifth, the task force recommended that third party data brokers buying and reselling people's information and data be required to register with the State, that meaningful tools be established for people to manage and control their data, including an opt-in or opt-out of the sale or use of their data by third parties, and that penalties be established for non-compliance.

Sixth, the task force recommended that, in order to align state law with the holding by the Supreme Court of the United States in Carpenter v. United States, 138 S.Ct. 2206 (2018), and current law enforcement practice, the Hawaii Revised Statutes should be amended to:

(1) Require law enforcement to obtain a search warrant before accessing a person's electronic communications in non-exigent or non-consensual circumstances; and

(2) Authorize governmental entities to request, and authorize courts to approve, the delay of notification of law enforcement access to electronic communications up to the deadline to provide discovery in criminal cases.

Lastly, the task force recommended that the State protect the privacy of a person's likeness by adopting laws that prohibit the unauthorized use of deep fake technology, which is improving rapidly, and easily sharable on social media.

Accordingly, the purpose of this Act is to implement the recommendations of the twenty-first century privacy law task force.

PART II

SECTION 2. Section 487N-1, Hawaii Revised Statutes, is amended as follows:

1. By adding two new definitions to be appropriately inserted and to read:

""Identifier" means a common piece of information related specifically to an individual, that is commonly used to identify that individual across technology platforms, including a first name or initial, and last name; a user name for an online account; a phone number; or an email address.

"Specified data element" means any of the following:

(1) An individual's social security number, either in its entirety or the last four or more digits;

(2) Driver's license number, federal or state identification card number, or passport number;

(3) A federal individual taxpayer identification number;

(4) An individual's financial account number or credit or debit card number;

(5) A security code, access code, personal identification number, or password that would allow access to an individual's account;

(6) Health insurance policy number, subscriber identification number, or any other unique number used by a health insurer to identify a person;

(7) Medical history, medical treatment by a health-care professional, diagnosis of mental or physical condition by a health care professional, or deoxyribonucleic acid profile;

(8) Unique biometric data generated from a measurement or analysis of human body characteristics used for authentication purposes, such as a fingerprint, voice print, retina or iris image, or other unique physical or digital representation of biometric data; and

(9) A private key that is unique to an individual and that is used to authenticate or sign an electronic record."

2. By amending the definition of "personal information" to read:

"Personal information" means an [~~individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:~~

~~(1) Social security number;~~

~~(2) Driver's license number or Hawaii identification card number; or~~

~~(3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.~~]

identifier in combination with one or more specified data elements. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."

PART III

SECTION 3. The Hawaii Revised Statutes is amended by adding a new chapter to title 26 to be appropriately designated and to read as follows:

"**CHAPTER**

CONSUMER PRIVACY

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 de-identified.

"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, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

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

"Business purpose" means the use of personal information for the business's operational purposes, or other notified purposes; provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. "Business purposes" include:

(1) Auditing related to a current interaction with the consumer and concurrent transactions, including counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards;

(2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity;

(3) Debugging to identify and repair errors that impair existing intended functionality;

(4) Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including the contextual customization of ads shown as part of the same interaction;

(5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider;

(6) Undertaking internal research for technological development and demonstration; and

(7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

"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.

"Commercial purpose" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. "Commercial purpose" does not include engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

"Consumer" means an individual residing in the State.

"Consumer reporting agency" shall have the same meaning as the federal Fair Credit Reporting Act (15 U.S.C. chapter 41 subchapter III).

"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 a business, or unit or units of a business, separately or together, that engages in:

(1) A one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; or

(2) A sale or license of data that is merely incidental to the business.

"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.

"Designated method for submitting requests" means a mailing address, email address, webpage, web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, or any other consumer-friendly means of contacting a business.

"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 is: a customer, client, subscriber, or user of the business's goods or services; employee, contractor, or agent of the business; investor in the business; or donor to the business. "Direct relationship" does not include the following activities conducted by a business, or the collection and sale or licensing of personal information incidental to conducting these activities:

(1) Developing or maintaining third-party e-commerce or application platforms;

(2) Providing directory assistance or directory information services, including name, address, and

telephone number, on behalf of or as a function of a telecommunications carrier;

(3) Providing publicly available information related to a consumer's business or profession; and

(4) Providing publicly available information via real-time or near real-time alert services for health or safety purposes.

"Family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

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

"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.

"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, email 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, a family, or a 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:

(1) 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; and

(2) That seeks disclosure of information described in section -11(a).

PART II. CONSUMER RIGHTS TO PERSONAL INFORMATION

§ -11 Right to request personal information; collection, disclosure, and delivery of personal information. (a) A consumer may request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected, including:

(1) The categories of personal information it has collected about that consumer;

(2) The categories of sources from which the personal information is collected;

(3) The business or commercial purpose for collecting or selling personal information;

(4) The categories of third parties with whom the business shares personal information;

(5) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold;

(6) The categories of personal information that the business disclosed about the consumer for a business purpose; and

(7) The specific pieces of personal information it has collected about that consumer.

(b) A business that collects a consumer's personal information, at or before the point of collection, shall inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

(c) A business shall provide the information specified in subsection (a) to a consumer only upon receipt of a verifiable consumer request.

(d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a twelve-month period.

(e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if the information is not sold or retained by the business or used to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

§ -12 Right to delete personal information. (a) A consumer may request that a business delete any personal information about the consumer that the business has collected from the consumer.

(b) A business that collects personal information about consumers shall disclose, pursuant to this section, the consumer's right to request the deletion of the consumer's personal information. A business that sells consumers' personal information to third parties shall disclose to consumers that their information may be sold and that consumers may request the deletion of their personal information.

(c) A business that receives a verifiable request from a consumer to delete the consumer's personal information pursuant to subsection (a) shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

(d) A business shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business to maintain the consumer's personal information to:

(1) Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise fulfill a contractual obligation between the business and the consumer;

(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity;

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

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

(5) Comply with section 803-47.6 or section 803-47.7;

(6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or

seriously impair the achievement of the research, if the consumer has provided informed consent;

(7) Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business;

(8) Comply with a legal obligation; or

(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

§ -13 Discrimination against consumers. (a) A business shall not discriminate against a consumer in response to the consumer's exercise of any of the consumer's rights under this part by:

(1) Denying goods or services to the consumer;

(2) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;

(3) Providing a different level or quality of goods or services to the consumer;

(4) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services; or

(5) Any other method of discouraging the consumer's patronage of the business.

(b) Nothing in this section prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's personal information.

(c) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's personal information.

§ -14 Obligations of a business. (a) When complying with requirements of this part, a business shall:

(1) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed, including, at a minimum, a toll-free telephone number, and if the business maintains a website, a website address; and

(2) Disclose and deliver the required information to a consumer free of charge within forty-five days of receiving a verifiable request from the consumer; provided that a business may take steps to determine whether the request is a verifiable request; provided further that time taken to determine whether a request is a verifiable request shall not extend the business's duty to disclose and deliver the information within forty-five days of receipt of the consumer's request.

(b) A business's disclosure of personal information shall:

(1) At a minimum, cover the twelve-month period preceding the business's receipt of the verifiable request; and

(2) Be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or

electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance.

(c) The time period to provide the required information may be extended once by an additional forty-five days when reasonably necessary if the consumer is provided notice of the extension within the first forty-five-day period.

(d) If a business does not take action on the request of a consumer, the business shall inform the consumer, without delay and within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(e) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the

burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.

(f) A business shall not require a consumer to create an account with the business in order to make a verifiable request.

(g) The obligations imposed on businesses by this part shall not restrict a business's ability to:

(1) Comply with federal, state, or local laws;

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, search warrant, or summons by federal, state, or local authorities;

(3) 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 local law;

(4) Exercise or defend legal claims;

(5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information; provided that with respect to deidentified information, the business shall:

(A) Have implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain;

(B) Have implemented business processes that specifically prohibit reidentification of the information;

(C) Have implemented business processes to prevent inadvertent release of deidentified information; and

(D) Make no attempt to reidentify the information; or

(6) Collect or sell a consumer's personal information if the business collected that information while the consumer was outside of the State, no part of the sale of the consumer's personal information occurred in the State, and no personal information collected is sold while the consumer was in the State; provided that this paragraph shall not be construed to authorize a business to:

(A) Store, regardless of whether the storage is on device, personal information about a consumer when the consumer is in the State; and

(B) Subsequently collect the aforementioned personal information when the consumer and stored personal information are outside of the State.

§ -15 Federal law exemptions. (a) This part shall not apply to protected health information that is collected by a covered entity governed by the chapter 323B or governed by the privacy, security, and breach notification rules issued by the federal Department of Health and Human Services, title 45 Code of Federal Regulations parts 160 and 164, established pursuant to the Health Insurance Portability and Availability Act of 1996 (P.L. 104-191).

(b) This part shall not apply to the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report as defined in title 15 United States Code section 1681a(d), and use of that information is limited by the federal Fair Credit Reporting Act (15 U.S.C. chapter 41 subchapter III).

(c) This part shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (P.L. 106-102), and implementing

regulations, to the extent this part is in conflict with that law.

§ -16 Enforcement; penalties. (a) A business that violates any provision of this part shall be subject to a fine of $7,500 for each offense.

(b) The attorney general may adopt rules pursuant to chapter 91 to implement the provisions of this section and to conduct civil investigations, enter into assurances of discontinuance, and bring civil actions as provided by law.

PART III. DATA BROKERS

§ -21 Annual registration. (a) Annually, on or before January 31, following a year in which a business meets the definition of data broker, a data broker shall:

(1) Register with the office of consumer protection;

(2) Pay a registration fee of $100; and

(3) Provide the following information to the office of consumer protection:

(A) The name and primary physical, e-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;

(D) A statement whether the data broker implements a purchaser credentialing process;

(E) The number of security breaches that the data broker has experienced during the prior year, and if known, the total number of consumers affected by the breaches;

(F) Where the data broker has actual knowledge that it possesses the personal information of minors, a separate statement detailing the data collection practices, databases, sales

activities, and opt-out policies that are applicable to the personal information of minors; and

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

(b) A data broker that fails to register shall be subject to the following:

(1) A civil penalty of $100 for each day it fails to register pursuant to this section;

(2) Pay the State an amount equal to the fees due under this section during the period the data broker failed to register pursuant to this section; and

(3) Other penalties imposed by law and reimbursement to the State for expenses incurred by the attorney general in the investigation and prosecution of the action, as the court deems appropriate.

(c) The attorney general may take legal action to collect or cause the collection of the penalties, fees and other moneys imposed in this section and to seek appropriate injunctive relief.

(d) The office of consumer protection shall create a page on its website where the information provided by data brokers under this title shall be accessible to the public.

§ -22 Duty to protect personal information. (a) A data broker shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to the:

(1) Size, scope, and type of business of the data broker obligated to safeguard the personal information under such comprehensive information security program;

(2) Amount of resources available to the data broker;

(3) Amount of stored data; and

(4) Need for security and confidentiality of personal information.

(b) A data broker subject to this part shall adopt safeguards in the comprehensive security program that are consistent with the safeguards for protection of personal information and information of a similar character set forth in other state rules or federal regulations applicable to the data

broker. A comprehensive information security program, at minimum, shall have the following features:

(1) Designation of one or more employees to maintain the program;

(2) Identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other records containing personal information, and a process for evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including:

(A) Ongoing employee training, including training for temporary and contract employees;

(B) Employee compliance with policies and procedures; and

(C) Means for detecting and preventing security system failures;

(3) Security policies for employees relating to the storage, access, and transportation of records containing personal information outside business premises;

(4) Disciplinary measures for violations of the comprehensive information security program rules;

(5) Measures that prevent terminated employees from accessing records containing personal information;

(6) Supervision of service providers, by:

(A) Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information consistent with applicable law; and

(B) Requiring third-party service providers by contract to implement and maintain appropriate security measures for personal information;

(7) Reasonable restrictions upon physical access to records containing personal information and storage of the records and data in locked facilities, storage areas, or containers;

(8) Regular monitoring to:

(A) Ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized

access to or unauthorized use of personal information; and

(B) Upgrade information safeguards as necessary to limit risks;

(9) Regular review of the scope of the security measures must occur:

(A) At least annually; or

(B) Whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information; and

(10) Documentation of responsive actions taken in connection with any incident involving a breach of security, and post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

§ -23 **Computer system security requirements.** A comprehensive information security program required by this part at a minimum, shall have the following elements, to the extent technically feasible:

(1) Secure user authentication protocols that have the following features:

(A) Control of user IDs and other identifiers;

(B) A reasonably secure method of assigning and selecting passwords or use of unique identifier technologies, such as biometrics or token devices;

(C) Control of data security passwords to ensure that such passwords are kept in a location and format that do not compromise the security of the data they protect;

(D) Restricting access to only active users and active user accounts; and

(E) Blocking access to user identification after multiple unsuccessful attempts to gain access;

provided that in lieu of the requirements, an authentication protocol providing a higher level of security may be used;

(2) Secure access control measures that:

(A) Restrict access to records and files containing personal information to those who need such information to perform their job duties; and

(B) Assign to each person with computer access unique identifications plus passwords, which are not vendor-supplied default passwords, that are reasonably designed to maintain the integrity of the security of the access controls or a protocol that provides a higher degree of security;

(3) Encryption of all transmitted records and files containing personal information that will travel across public networks and encryption of all data containing personal information to be transmitted wirelessly or a protocol that provides a higher degree of security;

(4) Reasonable monitoring of systems for unauthorized use of or access to personal information;

(5) Encryption of all personal information stored on laptops or other portable devices or a protocol that provides a higher degree of security;

(6) For files containing personal information on a system that is connected to the internet, reasonably up-to-date firewall protection and operating system security patches that are reasonably designed to maintain the integrity of the personal information or a protocol that provides a higher degree of security;

(7) Reasonably up-to-date versions of system security agent software that includes malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions and is set to receive the most current security updates on a regular basis or a protocol that provides a higher degree of security; and

(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

§ -24 Acquisition, use, and sale of personal information; prohibitions. (a) A person shall not acquire personal information through fraudulent means.

(b) A person shall not acquire or use personal information for the purpose of:

(1) Stalking or harassing another person;

(2) Committing a fraud, including identity theft, financial fraud, or email fraud; or

(3) Engaging in unlawful discrimination, including employment discrimination and housing discrimination.

(c) Any data broker that is not a consumer reporting agency shall establish a designated request process through which a consumer may submit a request pursuant to this part. A consumer, at any time, may submit a request through a designated request process to a data broker directing the data broker not to make any sale of any covered information the data broker has collected or will collect about the consumer.

(d) A data broker that has received a request submitted by a consumer shall not make any sale of any covered information the data broker has collected or will collect about that consumer.

(e) A data broker shall respond to a request submitted by a consumer within sixty days after receipt. A data broker may extend the foregoing period by not more than thirty days if the

data broker determines that the extension is reasonably necessary; provided that the data broker shall notify the consumer of the extension.

§ -25 Disclosures to consumers. (a) A data broker, upon request and proper identification of any consumer, shall clearly and accurately disclose to the consumer all information that the data broker has collected at the time of the request pertaining to the consumer, including:

(1) The categories of personal information it has shared about that consumer;

(2) The categories of sources from which the personal information is collected;

(3) The names of third parties with whom the data broker has shared personal information during the prior twelve-month period and the date of each request; and

(4) The specific pieces of personal information it has shared about that consumer.

(b) A data broker may provide disclosure to a consumer at any time, but shall not be required to provide disclosure to a consumer more than twice in a twelve-month period.

(c) Consumer reporting agencies that broker data of residents of the State shall annually provide a written notice to consumers, in at least twelve-point type, containing the following information:

(1) The circumstances under which a consumer has the right to receive a free copy of their credit report and the methods for obtaining the report;

(2) The circumstances under which a person may access another person's credit report without their permission, such as in response to a court order, or direct mail offers of credit;

(3) An explanation of a security freeze, along with the circumstances under which the consumer has the right to place a "security freeze" on a credit report, and the costs and process for placing the freeze; and

(4) Notice that if the consumer believes a law regulating consumer credit reporting has been violated, the consumer may file a complaint with the Federal Trade Commission, with the processes for filing the complaint.

§ -26 Discrimination against consumers. (a) A business shall not discriminate against a consumer in response to the consumer's exercise of any of the consumer's rights under this part by:

(1) Denying goods or services to the consumer;

(2) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;

(3) Providing a different level or quality of goods or services to the consumer;

(4) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services; or

(5) Any other method of discouraging the consumer's patronage of the business.

(b) Nothing in this section prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.

(c) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's data.

§ -27 Enforcement; penalties. (a) A person who violates a provision of this part, other than section -21, shall have committed a deceptive business act under section 480-2.

(b) The attorney general may adopt rules to implement the provisions of this section and to conduct civil investigations, enter into assurances of discontinuance, and bring civil actions as provided by law."

PART IV

SECTION 4. Chapter 481B, Hawaii Revised Statutes, is amended by adding two new sections to part I to be appropriately designated and to read as follows:

"**§481B- Sale of geolocation information without consent is prohibited.** (a) No person, in any manner, or by any means,

shall sell or offer for sale geolocation information that is recorded or collected through any means by mobile devices or location-based applications without the explicit consent of the individual who is the primary user of the device or application.

(b) As used in this section:

"Consent" means prior express opt-in authorization that may be revoked by the user at any time.

"Geolocation information" means information that is:

(1) Not the contents of a communication;

(2) Generated by or derived from, in whole or in part, the operation of a mobile device, including, but not limited to, a smart phone, tablet, fitness tracker, e-reader, or laptop computer; and

(3) Sufficient to determine or infer the precise location of the user of the device.

"Location-based application" means a software application that is downloaded or installed onto a device or accessed via a web browser and collects, uses, or stores geolocation information.

"Precise location" means any data that locates a user within a geographic area that is equal to or less than the area of a circle with a radius of one mile.

"Sale" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a user's geolocation information to another business or a third party for monetary or other valuable consideration.

"User" means a person who purchases or leases a device or installs or uses an application on a mobile device.

§481B- Sale of internet browser information without consent is prohibited. (a) No person, in any manner, or by any means, shall sell or offer for sale internet browser information without the explicit consent of the subscriber of the internet service.

(b) As used in this section:

"Consent" means prior express opt-in authorization which may be revoked by the subscriber at any time.

"Internet service" means a retail service that provides the capability to transmit data to and receive data through the internet using a dial-up service, a digital subscriber line,

cable modem, fiber optics, wireless radio, satellite, or powerline, or other technology used for a similar purpose.

"Internet browser information" means information from a person's use of the internet, including:

(1) Web browsing history;

(2) Application usage history;

(3) The origin and destination Internet protocol addresses;

(4) A device identifier, such as a media access control address, international mobile equipment identity, or Internet protocol addresses; and

(5) The content of the communications comprising the internet activity.

"Sale" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, internet browser information to another business or a third party for monetary or other valuable consideration.

"Subscriber" means an applicant for or a current or former customer of an internet service."

PART V

SECTION 5. Section 803-41, Hawaii Revised Statutes, is amended by adding a new definition to part IV to be appropriately inserted and to read as follows:

""Electronically stored data" means any information that is recorded, stored, or maintained in electronic form by an electronic communication service or a remote computing service. "Electronically stored data" includes the contents of communications, transactional records about communications, and records and information that relate to a subscriber, customer, or user of an electronic communication service or a remote computing service."

SECTION 6. Section 803-47.6, Hawaii Revised Statutes, is amended to read as follows:

"**§803-47.6 Requirements for governmental access.** (a) [~~A~~] Except as otherwise provided by law, a governmental entity may require [~~the disclosure by~~] a provider of an electronic communication service [~~of the contents of an electronic communication~~] and a provider of a remote computing service to disclose electronically stored data pursuant to a search warrant

[~~only.~~] or written consent from the customer, subscriber, or user of the service.

[~~(b) A governmental entity may require a provider of remote computing services to disclose the contents of any electronic communication pursuant to a search warrant only.~~

~~(c) Subsection (b) of this section is applicable to any electronic communication held or maintained on a remote computing service:~~

~~(1) On behalf of, and received by electronic transmission from (or created by computer processing of communications received by electronic transmission from), a subscriber or customer of the remote computing service; and~~

~~(2) Solely for the purpose of providing storage or computer processing services to the subscriber or customer, if the provider is not authorized to access the contents of those communications for any purpose other than storage or computer processing.~~

~~(d) (1) A provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to, or~~

~~customer of, the service (other than the contents of any electronic communication) to any person other than a governmental entity.~~

~~(2) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to, or customer of, the service (other than the contents of an electronic communication) to a governmental entity only when:~~

~~(A) Presented with a search warrant;~~

~~(B) Presented with a court order, which seeks the disclosure of transactional records, other than real-time transactional records;~~

~~(C) The consent of the subscriber or customer to the disclosure has been obtained; or~~

~~(D) Presented with an administrative subpoena authorized by statute, an attorney general subpoena, or a grand jury or trial subpoena, which seeks the disclosure of information concerning electronic communication, including but not limited to the name, address, local and~~

~~long-distance telephone billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of the service, and the types of services the subscriber or customer utilized.~~

~~(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.~~

~~(c) A court order for disclosure under subsection (d) shall issue only if the governmental entity demonstrates probable cause that the records or other information sought, constitute or relate to the fruits, implements, or existence of a crime or are relevant to a legitimate law enforcement inquiry. An order may be quashed or modified if, upon a motion promptly made, the service provider shows that compliance would be unduly burdensome because of the voluminous nature of the information or records requested, or some other stated reason establishing such a hardship.~~]

(b) Unless otherwise authorized by the court, a governmental entity receiving records or information under this

section shall provide notice to the subscriber, customer, or user of the service.

[~~(f)~~] (c) No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, or subpoena.

[~~(g)~~] (d) A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a [~~court order or other process.~~] search warrant. Records shall be retained for a period of ninety days, which shall be extended for an additional ninety-day period upon a renewed request by the governmental entity."

SECTION 7. Section 803-47.7, Hawaii Revised Statutes, is amended as follows:

1. By amending subsection (a) to read

"(a) A governmental entity may include in its [~~court order~~] search warrant a requirement that the service provider

create a backup copy of the contents of the electronic communication without notifying the subscriber or customer. The service provider shall create the backup copy as soon as practicable, consistent with its regular business practices, and shall confirm to the governmental entity that the backup copy has been made. The backup copy shall be created within two business days after receipt by the service provider of the [~~subpoena or court order.~~] warrant."

2. By amending subsection (e) to read:

"(e) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (b) of this section, the subscriber or customer may file a motion to vacate the [~~court order,~~] search warrant, with written notice and a copy of the motion being served on both the governmental entity and the service provider. The motion to vacate a [~~court order~~] search warrant shall be filed with the designated judge who issued the [~~order.~~] warrant. The motion or application shall contain an affidavit or sworn statement:

(1) Stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications are sought; and

(2) Setting forth the applicant's reasons for believing that the records sought does not constitute probable cause or there has not been substantial compliance with some aspect of the provisions of this part."

3. By amending subsection (g) to read:

"(g) If the court finds that the applicant is not the subscriber or customer whose communications are sought, or that there is reason to believe that the law enforcement inquiry is legitimate and the justification for the communications sought is supported by probable cause, the application or motion shall be denied, and the court shall order the release of the backup copy to the government entity. A court order denying a motion or application shall not be deemed a final order, and no interlocutory appeal may be taken therefrom by the customer. If the court finds that the applicant is a proper subscriber or customer and the justification for the communication sought is not supported by probable cause or that there has not been substantial compliance with the provisions of this part, it shall order vacation of the [~~order~~] warrant previously issued."

SECTION 8. Section 803-47.8, Hawaii Revised Statutes, is amended as follows:

1. By amending subsection (a) to read:

"(a) A governmental entity may as part of a request for a [~~court order~~] search warrant to include a provision that notification be delayed for a period not exceeding ninety days or, at the discretion of the court, no later than the deadline to provide discovery in a criminal case, if the court determines that notification of the existence of the court order may have an adverse result."

2. By amending subsection (c) to read:

"(c) Extensions of delays in notification may be granted up to ninety days per application to a court[~~.~~] or, at the discretion of the court, up to the deadline to provide discovery in a criminal case. Each application for an extension must comply with subsection (e) of this section."

3. By amending subsection (e) to read:

"(e) A governmental entity may apply to the designated judge or any other circuit judge or district court judge, if a circuit court judge has not yet been designated by the chief justice of the Hawaii supreme court, or is otherwise unavailable, for an order commanding a provider of an electronic communication service or remote computing service to whom a

search warrant, or court order is directed, not to notify any other person of the existence of the search warrant [~~, or court order~~] for such period as the court deems appropriate not to exceed ninety days [~~.~~] or, at the discretion of the court, no later than the deadline to provide discovery in a criminal case. The court shall enter the order if it determines that there is reason to believe that notification of the existence of the search warrant [~~, or court order~~] will result in:

(1) Endangering the life or physical safety of an individual;

(2) Flight from prosecution;

(3) Destruction of or tampering with evidence;

(4) Intimidation of potential witnesses; or

(5) Otherwise seriously jeopardizing an investigation or unduly delaying a trial."

PART VI

SECTION 9. Section 711-1110.9, Hawaii Revised Statutes, is amended to read as follows:

"**§711-1110.9 Violation of privacy in the first degree.** (1) A person commits the offense of violation of privacy in the

first degree if, except in the execution of a public duty or as authorized by law:

(a) The person intentionally or knowingly installs or uses, or both, in any private place, without consent of the person or persons entitled to privacy therein, any device for observing, recording, amplifying, or broadcasting another person in a stage of undress or sexual activity in that place; [~~or~~]

(b) The person knowingly discloses or threatens to disclose an image or video of another identifiable person either in the nude, as defined in section 712-1210, or engaging in sexual conduct, as defined in section 712-1210, without the consent of the depicted person, with intent to harm substantially the depicted person with respect to that person's health, safety, business, calling, career, education, financial condition, reputation, or personal relationships or as an act of revenge or retribution; [~~provided that:~~] or

(c) The person intentionally creates or discloses, or threatens to disclose, an image or video of a fictitious person depicted in the nude, as defined in

section 712-1210, or engaged in sexual conduct, as defined in section 712-1210, that includes the recognizable physical characteristics of a known person so that the image or video appears to depict the known person and not a fictitious person, with intent to harm substantially the depicted person with respect to that person's health, safety, business, calling, career, education, financial condition, reputation, or personal relationships, or as an act or revenge or retribution.

[~~(i)~~] (2) This [~~paragraph~~] section shall not apply to images or videos of the depicted person made:

[~~(A)~~] (a) When the person was voluntarily nude in public or voluntarily engaging in sexual conduct in public; or

[~~(B)~~] (b) Pursuant to a voluntary commercial transaction[~~; and~~].

[~~(ii)~~] (3) Nothing in this [~~paragraph~~] section shall be construed to impose liability on a provider of "electronic communication service" or "remote computing service" as those terms are defined in section 803-41, for an image or video

disclosed through the electronic communication service or remote computing service by another person.

[~~(2)~~] (4) Violation of privacy in the first degree is a class C felony. In addition to any penalties the court may impose, the court may order the destruction of any recording made in violation of this section.

[~~(3)~~] (5) Any recording or image made or disclosed in violation of this section and not destroyed pursuant to subsection [~~(2)~~] (4) shall be sealed and remain confidential."

PART VII

SECTION 10. This Act does not affect rights and duties that matured, penalties that were incurred, and proceedings that were begun before its effective date.

SECTION 11. Statutory material to be repealed is bracketed and stricken. New statutory material is underscored.

SECTION 12. This Act shall take effect upon its approval; provided that part III shall take effect on January 1, 2022.

H.B. NO. 2572 H.D. 1

Report Title:
Privacy; Office of Consumer Protection; Attorney General; Personal Information; Right to Deletion; Data Brokers; Geolocation Information; Search Warrants; Notice; Deep Fakes

Description:
Redefines "personal information" for the purposes of security breach of personal information law. Establishes new provisions on consumer rights to personal information and data brokers. Prohibits the sale of geolocation information and internet browser information without consent. Amends provisions relating to electronic eavesdropping law. Prohibits certain manipulated images of individuals. (HB2572 HD1)

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