THE SENATE
THIRTY-FIRST LEGISLATURE, 2021
STATE OF HAWAII

S.B. NO. 1009

JAN 27 2021

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, Regular Session of 2019, established the twenty-first century privacy law task force, whose membership consisted of individuals in government and the private sector having 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 that 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 have considered comprehensive privacy legislation in recent legislative sessions.

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

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487N, Hawaii Revised Statutes, should be updated and expanded, as the current definition of "personal information" is outdated. 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.

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 raise 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.

The task force also 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.

The task force further 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 entities 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~~] shall not include

publicly available information that is lawfully made available to the general public from federal, state, or local government records."

SECTION 3. Section 487N-2, Hawaii Revised Statutes, is amended by amending subsection (g) to read as follows:

"(g) The following businesses shall be deemed to be in compliance with this section:

(1) A financial institution that is subject to the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice published in the Federal Register on March 29, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, or subject to 12 C.F.R. Part 748, and any revisions, additions, or substitutions relating to the interagency guidance; and

(2) Any health plan or healthcare provider and its business associates that [~~is~~] are subject to and in compliance with the standards for privacy or

individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996."

PART III

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 a mobile device or location-based application 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.

"Emergency" means the imminent or actual occurrence of an event that is likely to cause extensive injury, death, or property damage.

"Geolocation information" means information that is:

(1) Not the contents of a communication;

(2) Generated by or derived, in whole or in part, from 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 that 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 having 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. "Sale" shall not include the releasing, disclosing, disseminating, making available, transferring, or otherwise

communicating orally, in writing, or by electronic or other means, a user's geolocation information for the purpose of responding to an emergency.

"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 that may be revoked by the subscriber at any time.

"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.

"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, powerline, or other technology used for a similar purpose.

"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 IV

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

1 ""Electronically stored data" means any information that is
2 recorded, stored, or maintained in electronic form by an
3 electronic communication service or a remote computing service.
4 "Electronically stored data" includes the contents of
5 communications, transactional records about communications, and
6 records and information that relate to a subscriber, customer,
7 or user of an electronic communication service or a remote
8 computing service."
9 SECTION 6. Section 803-47.6, Hawaii Revised Statutes, is
10 amended to read as follows:
11 "**§803-47.6 Requirements for governmental access.** (a) [~~A~~]
12 Except as otherwise provided by law, a governmental entity may
13 require [~~the disclosure by~~] a provider of an electronic
14 communication service [~~of the contents of an electronic~~
15 ~~communication~~] and a provider of a remote computing service to
16 disclose electronically stored data pursuant to a search warrant
17 [~~only.~~] or written consent from the customer, subscriber, or
18 user of the service.
19 [~~(b) A governmental entity may require a provider of~~
20 ~~remote computing services to disclose the contents of any~~
21 ~~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.~~

~~(e) 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 V

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 VI

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.

INTRODUCED BY: _____

S.B. NO. 1009

Report Title:
Privacy; Attorney General; Personal Information; Geolocation Information; Search Warrants; Notice; Deep Fakes

Description:
Amends the definition of "personal information" for the purpose of applying modern security breach of personal information law. 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.

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