HOUSE OF REPRESENTATIVES
THIRTIETH LEGISLATURE, 2020
STATE OF HAWAII

H.B. NO. 2572 H.D. 2 S.D. 1 Proposed

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 S.D.1, Regular Session of 2019 ("resolution") established the twenty-first century privacy law task force ("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 privacy legislation during their current legislative sessions.

Following significant inquiry and discussion, the task force made various recommendations on issues such as: modernizing the definition of personal information as it relates to data breaches and the nonconsensual sale of a person's data such as geolocation information.

The legislature further finds that in early 2020, governmental and societal responses to the COVID-19 pandemic changed typical types of human interaction. As residents have been mandated and encouraged to stay at home to prevent infection and the spread of COVID-19, an increased online presence has become the new normal. Residents have been forced to use digital methods to shop for groceries and household items, attend classes, complete work projects, and engage in

other activity that could usually be done through a non-digital means. Often times these online activities require users to create accounts and share personal information. These online activities also require many businesses to protect a larger volume and new types of data than before, making them potential targets for those looking to steal personal information and data for nefarious purposes.

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. The types of personal information collected by companies online has grown significantly since chapter 487N, Hawaii Revised Statutes, was enacted, and the ways that bad actors can use that information has grown as well. There are 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 comprehensive enough, as presently written, to cover the additional identifiers. Especially in light of increased digital activity

users engage in because of the COVID-19 pandemic, the definition of "personal information" in chapter 487N, Hawaii Revised Statutes, should be updated and expanded to include various personal identifiers and data elements that are found in more comprehensive laws.

Additionally, the high transmissibility of the COVID-19 virus has lead businesses and governments to consider and implement ways to contact trace people that may have been exposed to the virus. Certain proposed methods of contact tracing have included using geolocation data.

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 arisen 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. Residents of Hawaii should be able to share their geolocation data to help limit the spread of the novel coronavirus, without sacrificing their privacy or safety.

Accordingly, the purpose of this Act is to protect Hawaii residents and their personal data in a digital-focused COVID-19 society by implementing certain 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, when the specified data element or elements are not encrypted. "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 a new section 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.

"Emergency" means the imminent or actual occurrence of an event, which has the likelihood of causing extensive injury, death, or property damage. "Emergency" shall not include the spread of a bacteria or virus.

"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. "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."

PART IV

SECTION 5. This Act does not affect rights and duties that matured, penalties that were incurred, and proceedings that were begun before its effective date.

SECTION 6. Statutory material to be repealed is bracketed and stricken. New statutory material is underscored.

SECTION 7. This Act shall take effect upon its approval.

H.B. NO. 2572 H.D. 2 S.D. 1 Proposed

Report Title:
Privacy; Personal Information; Geolocation Information

Description:
Modernizes "personal information" for the purposes of security breach of personal information law. Prohibits the sale of geolocation information without consent. (Proposed SD1)

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