Information Privacy and Security Council
Meeting Agenda - Amended
July 15, 2020
1:00 p.m.

Virtual Meeting via Webex

Members of the public may join the meeting by clicking on the link. To request the passcode, please email ets@hawaii.gov .
https://fedgovdemo.webex.com/fedgovdemo/onstage/g.php?MTID=e75d89271d7ae032043b8591adc013ed7

I. Call to Order

II. Review and Approval of the December 18, 2019 Meeting Minutes

III. Public Testimony on Agenda Items

Any person may submit testimony on any agenda item. Due to the safer-at-home orders, members of the public may submit written testimony or submit oral testimony via e-mail to ets@hawaii.gov, Subject line: IPSC Testimony. Each individual or representative of an organization is allotted three minutes for testimony.

IV. House Bill 2572, Relating to Privacy (attached); Discussion and Appropriate Action

V. Personal Information System Annual Report; Discussion and Appropriate Action

VI. IT Internal Security Controls

The Council anticipates going into executive session pursuant to HRS section 92-5(a)(6) to consider sensitive matters relating to IT internal security controls.

VII. Good of the Order
   a. Announcements
   b. Next meeting: August 19, 2020

VIII. Adjournment

Information Privacy and Security Council (IPSC)
Meeting Minutes - DRAFT
December 18, 2019

Videoconference Centers (VCC)
Kalanimoku Bldg., 1151 Punchbowl St., Basement B-10, Honolulu, HI 96813
Hilo State Office Bldg., 75 Aupuni St., Basement, Hilo, HI 96720
Wailuku State Office Bldg., 54 S. High St., 3rd Flr., Wailuku, HI 96793
Lihue State Office Bldg., 3060 Eiwa St., Basement, Lihue, HI 96766

Members Present

Vince Hoang, Acting Chair	Office of Enterprise Technology Services (ETS)
Robert Strickland (Designee)	Department of Education (DOE), via VCC Maui*
Gino Merez	Department of Health (DOH)
David Keane	Department of Human Resources Development (DHRD)
Lim Yong	Department of Human Services (DHS)
Kevin Thornton	Judiciary
Jodi Ito (Designee)	University of Hawai‘i (UH)
Karen Sherman	County of Maui, via VCC*
Nyree Norman	County of Kauai, via VCC*
Jules Ung	County of Hawai‘i, via VCC*

* The neighbor island members participated by video and telephone conference.

Members Absent

Stephen Levins	Department of Commerce and Consumer Affairs (DCCA)
Carol Taniguchi	Legislature
Mark Wong	City & County of Honolulu

Other Attendees

Valri Kunimoto	Department of the Attorney General (ATG)
Lori Tanigawa	Department of the Attorney General (ATG)
Kelly McCanlies	Hawaiian Electric Co.
Landon Wong	HPPA

I. Call to Order

Acting Chair Hoang called the meeting to order at 1:11 p.m., at which time quorum was established.

II. Review and Approval of the November 20, 2019 Meeting Minutes

Member Thornton made a motion to approve the November 20, 2019 meeting minutes, which was seconded by Member Keane. A vote was taken and the motion passed unanimously.

III. Public Testimony on Agenda Items

None.

IV. House Concurrent Resolution 225, Twenty-first Century Privacy Law Task Force

The Task Force is considering legislation to revise Chapter 487N, Hawaii Revised Statutes (HRS), concerning the confidentiality of personal information.

Acting Chair Hoang invited Kelly McCanlies, a member of the Task Force, to the meeting. She stated that the Task Force was chaired by Representative Chris Lee and Senator Michelle Kidani. Meetings began in August 2019 and had its last meeting in November. Groups of members worked on ideas that the Task Force wanted to pursue. There are about seven pieces of legislation that were produced by the Task Force but we don't know if all will be introduced. The Task Force's highest priority was revising Chapter 487N, HRS, Security Breach of Personal Information. She shared a draft of the proposed legislation that she will be sending to the Task Force. Most states have updated their laws regarding data breach notification laws, whereas Hawaii has not. She asked the Committee for their input.

Members gave different scenarios asking if the proposed legislation would trigger a data breach. Members questioned whether the definition of an Identifier will erroneously trigger data breach reports. Member Designee Ito felt that the definitions for an Identifier, such as phone number or email address were too broad and most could be considered public information. Ms. McCanlies explained that an Identifier could be used to tie different pieces of information together, which is why its listed that way. She also noted that the current statute also addresses "risk of harm to a person" under the definition of "security breach" so an Identifier with a data element would not automatically be a data breach.

Members subject to HIPAA (Health Insurance Portability and Accountability Act) asked how the proposed changes would affect their reporting when there is a data breach. Ms. McCanlies stated that the current law addresses that issue under Chapter 487N-2(g)2.

Ms. McCanlies stated that about two-thirds of the data breach notification laws have been changed to be more inclusive. Medical identity theft has increased exponentially. The Task Force committee discussed device Identifiers but decided not to include it. It is being considered at the federal level as the Federal Trade Commission stated that device identifiers and especially IP address are now considered personal information.

She plans to submit the proposed draft to the Task Force on Friday. The members can send her an email with their comments before then. Member Thornton recommended changing the last four digits of a Social Security Number to six digits.

V. Good of the Order

a. Announcements: The IPSC will take a recess in January 2020.
b. Next meeting: February 19, 2020

VI. Adjournment

At 2:04 p.m., Member Yong made a motion to adjourn, which was seconded by Member Designee Ito. A vote was taken and the motion passed unanimously.

Recorded by: _____
Susan Bannister, ETS

HOUSE OF REPRESENTATIVES
THIRTIETH LEGISLATURE, 2020
STATE OF HAWAII

H.B. NO. 2572 H.D. 2 S.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 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 have 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. California has enacted a comprehensive privacy act and dozens of other states have already adopted components of the privacy law contained in this Act.

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 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.

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 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 led 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. Residents of Hawaii should be able to share their contact tracing information with authorized parties to help limit the spread of the novel coronavirus, without sacrificing their privacy or safety.

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 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 advancing rapidly, and easily sharable on social media.

Accordingly, the purpose of this Act is to protect Hawaii residents and their personal data in a digitally-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 first name or initial, and last name.

"Specified data element" means any of the following:

(1) An individual's social security number;

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

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

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

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

(8) 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 or otherwise rendered unreadable. "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 contact tracing information without consent is prohibited.** (a) No person or state agency, in any manner, or by any means, shall sell or offer for sale contact tracing information that is recorded or collected without the consent of the individual who is the primary user of the device or application.

(b) This section shall not apply to any activity involving the collection, maintenance, disclosure, sale, communication, or use of geolocation information to detect security incidents; protect against malicious, deceptive, fraudulent, or illegal activity; or to prosecute those responsible for that activity.

(c) As used in this section:

"Consent" means a clear affirmative act signifying a freely given, specific, informed, and unambiguous indication of a

user's agreement, such as by written statement, including by electronic means, or other clear affirmative action.

"Contact tracing information" means information that is:

(1) 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;

(2) Sufficient to determine or infer the location of the identifiable user of the device with precision and accuracy below one thousand seven hundred fifty feet; and

(3) Gathered for the purpose of identifying users who were in contact with a person who has tested positive for COVID-19 or was likely exposed to COVID-19.

"Contact tracing information" relates only to information collected following the effective date of this Act. "Contact tracing information" does not include information collected by an employer for the purposes of ensuring workplace, employee, or customer safety with regard to identifying and limited the spread of COVID-19.

"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.

"Sale" means the exchange of a user's contact tracing information for monetary consideration. The term "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 contact tracing information for the purpose of responding to an emergency or a pandemic. The term "sale" shall not include the transfer of a user's contact tracing information to a service provider who processes the contact tracing data on behalf of the user.

"Service provider" means any legal entity that collects or processes contact tracing data at the discretion of a state agency or user.

"User" means a person who purchases or leases a device or installs or uses an application on a mobile device and is a resident of Hawaii."

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:

""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.~~] search 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~~] search 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~~] warrant 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 substantially harm 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 on September 1, 2020, and shall be repealed on September 1, 2025; provided that sections 2 through 9 of this Act shall be reenacted in the form in which they read on the day before the effective date of this Act.

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

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

Description:
Modernizes "personal information" for the purposes of security breach of personal information law. Prohibits the sale of contact tracing information without consent. Amends provisions relating to electronic eavesdropping law. Prohibits certain manipulated images of individuals. Effective 9/1/2020. Sunsets 9/1/2025. (SD1)

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