



Information Privacy and Security Council

Meeting Agenda
September 16, 2020

1:00 p.m.

Virtual Meeting via Webex

Members of the public may request the virtual meeting link by e-mailing: ets@hawaii.gov, subject line: "IPSC Meeting", by September 15, 2020, 11:00 a.m.

- I. Call to Order
- II. Review and Approval of the July 15, 2020 Meeting Minutes
- III. Public Testimony on Agenda Items

Any person may submit testimony on any agenda item. Due to the stay-at-home/work-from-home order, 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; Discussion and Appropriate Action
- V. Personal Information System Annual Report; Discussion and Appropriate Action
- VI. Good of the Order
 - a. Announcements
 - b. Next meeting: November 18, 2020
- VII. Adjournment



**Information Privacy and Security Council (IPSC)
Meeting Minutes - DRAFT
July 15, 2020**

Videoconference meeting via Webex

Members Present

Vince Hoang, Acting Chair	Office of Enterprise Technology Services (ETS)
David Shak	Department of Commerce and Consumer Affairs (DCCA)
Gino Merez	Department of Health (DOH)
David Keane	Department of Human Resources Development (DHRD)
Louis "Jack" Giardina	Department of Human Services (DHS)
Kevin Thornton	Judiciary
Jodi Ito	University of Hawai'i (UH)
Karen Sherman	County of Maui
Nyree Norman	County of Kaua'i
Jules Ung	County of Hawai'i

Members Excused

	Department of Education (DOE)
Carol Taniguchi	Legislature
Mark Wong	City & County of Honolulu

Other Attendees

Candace Park	Department of the Attorney General (ATG)
Erin Nakama	ETS
Susan Bannister	ETS

I. Call to Order

Quorum was established and Acting Chair Hoang called the meeting to order at 1:11 p.m.

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

Acting Chair Hoang called for a motion to approve the minutes. Member Ito made a motion to approve the meeting minutes, which was seconded by Member Thornton. The motion passed unanimously.

III. Public Testimony on Agenda Items

None.

IV. House Bill 2572 HD2 SD1, Relating to Privacy

Acting Chair Hoang participated on the task force on behalf of the state CIO. The task force recommended that the definition of “personal information” in Chapter 487N, Hawaii Revised Statutes (HRS) be updated and expanded to include various personal identifiers and data elements. HB 2572 HD2 SD1 did not pass this legislative session. Hoang felt that the bill might have been too broad and tried to do much and asked members if the bill should be revised. Member Sherman stated that she is willing to review the bill and legislature comments if given time. The Committee will recess in August and meet in September to discuss her findings.

V. Personal Information System Annual Report

Acting Chair Hoang stated that no changes will be made to the Annual Personal Information System Report, Privacy Impact Assessment form. He will prepare a memo to government agencies reminding them of the September 30 deadline per 487N-7 HRS.

VI. IT Internal Security Controls

Pursuant to HRS section 92-5(a)(6) to consider sensitive matters relating to IT internal security controls, at 1:41 p.m., Acting Chair Hoang made a motion to move into executive session, which was seconded by Member Ito. The motion passed unanimously.

The IPSC exited executive session at 2:00 p.m.

VII. Good of the Order

- a. Next meeting: September 16, 2020. The IPSC will take a recess in August and resume in September.

VIII. Adjournment

Member Ito made a motion to adjourn, which was seconded by Member Shak. The motion passed unanimously.

Recorded by: _____
Susan Bannister, ETS

A BILL FOR AN ACT

RELATING TO PRIVACY.

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

1 PART I

2 SECTION 1. The legislature finds that House Concurrent
3 Resolution No. 225 S.D.1, Regular Session of 2019 ("resolution")
4 established the twenty-first century privacy law task force
5 ("task force"), whose membership consisted of individuals in
6 government and the private sector with an interest or expertise
7 in privacy law in the digital era. The resolution found that
8 public use of the internet and related technologies have
9 significantly expanded in recent years, and that a lack of
10 meaningful government regulation has resulted in personal
11 privacy being compromised. Accordingly, the legislature
12 requested that the task force examine and make recommendations
13 regarding existing privacy laws and regulations to protect the
14 privacy interests of the people of Hawaii.

15 The legislature further finds that the task force
16 considered a spectrum of related privacy issues which have been
17 raised in Hawaii and other states in recent years. Numerous



1 states have begun to address the heightened and unique privacy
2 risks that threaten individuals in the digital era of the
3 twenty-first century. California has enacted a comprehensive
4 privacy act and dozens of other states have already adopted
5 components of the privacy law contained in this Act.

6 The legislature further finds that in early 2020,
7 governmental and societal responses to the COVID-19 pandemic
8 changed typical types of human interaction. As residents have
9 been mandated and encouraged to stay at home to prevent
10 infection and the spread of COVID-19, an increased online
11 presence has become the new normal. Residents have been forced
12 to use digital methods to shop for groceries and household
13 items, attend classes, complete work projects, and engage in
14 other activity that could usually be done through non-digital
15 means. Often times these online activities require users to
16 create accounts and share personal information. These online
17 activities also require many businesses to protect a larger
18 volume and new types of data than before, making them potential
19 targets for those looking to steal personal information and data
20 for nefarious purposes.



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

6 The task force recommended that the definition of "personal
7 information" in chapter 487N, Hawaii Revised Statutes, should be
8 updated and expanded, as the current definition of "personal
9 information" is outdated and needs to be amended. The types of
10 personal information collected by companies online has grown
11 significantly since chapter 487N, Hawaii Revised Statutes, was
12 enacted, and the ways that bad actors can use that information
13 has grown as well. There are many identifying data elements
14 that, when exposed to the public in a data breach, place an
15 individual at risk of identity theft or may compromise the
16 individual's personal safety. Chapter 487N, which requires the
17 public to be notified of data breaches, is not comprehensive
18 enough, as presently written, to cover the additional
19 identifiers. Especially in light of increased digital activity
20 users engage in because of the COVID-19 pandemic, the definition
21 of "personal information" in chapter 487N, Hawaii Revised



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

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

9 The task force recommended that explicit consent be
10 required before an individual's geolocation data may be shared
11 or sold to a third party. Residents of Hawaii should be able to
12 share their contact tracing information with authorized parties
13 to help limit the spread of the novel coronavirus, without
14 sacrificing their privacy or safety.

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



- 1 "Identifier" means a first name or initial, and last name.
- 2 "Specified data element" means any of the following:
- 3 (1) An individual's social security number;
- 4 (2) Driver's license number, federal or state
5 identification card number, or passport number;
- 6 (3) A federal individual taxpayer identification number;
- 7 (4) An individual's financial account number or credit or
8 debit card number; security code, access code,
9 personal identification number, or password that would
10 allow access to an individual's account;
- 11 (5) Health insurance policy number, subscriber
12 identification number, or any other unique number used
13 by a health insurer to identify a person;
- 14 (6) Medical treatment by a health care professional,
15 diagnosis of mental or physical condition by a health
16 care professional, or deoxyribonucleic acid profile;
- 17 (7) Unique biometric data generated from a measurement or
18 analysis of human body characteristics used for
19 identification purposes, such as a fingerprint, voice
20 print, retina or iris image, or other unique physical
21 or digital representation of biometric data; and



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

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

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

9 ~~(1) Social security number,~~

10 ~~(2) Driver's license number or Hawaii identification card~~
11 ~~number, or~~

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

15 identifier in combination with one or more specified data
16 elements, when the specified data element or elements are not
17 encrypted or otherwise rendered unreadable. "Personal

18 information" ~~does~~ shall not include publicly available
19 information that is lawfully made available to the general
20 public from federal, state, or local government records."



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

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

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

16 (2) Any health plan or healthcare provider and its
17 business associates that [~~is~~] are subject to and in
18 compliance with the standards for privacy or
19 individually identifiable health information and the
20 security standards for the protection of electronic



1 health information of the Health Insurance Portability
2 and Accountability Act of 1996."

3 PART III

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

7 "§481B- Sale of contact tracing information without
8 consent is prohibited. (a) No person or state agency, in any
9 manner, or by any means, shall sell or offer for sale contact
10 tracing information that is recorded or collected without the
11 consent of the individual who is the primary user of the device
12 or application.

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

18 (c) As used in this section:

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



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

3 "Contact tracing information" means information that is:

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

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

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

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



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

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

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

14 **"§803-47.6 Requirements for governmental access. (a) [A]**
15 Except as otherwise provided by law, a governmental entity may
16 require [the disclosure by] a provider of an electronic
17 communication service [of the contents of an electronic
18 communication] and a provider of a remote computing service to
19 disclose electronically stored data pursuant to a search warrant
20 [only.] or written consent from the customer, subscriber, or
21 user of the service.



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

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

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

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

17 ~~(d)(1) A provider of electronic communication service or~~
18 ~~remote computing service may disclose a record or~~
19 ~~other information pertaining to a subscriber to, or~~
20 ~~customer of, the service (other than the contents of~~



1 ~~any electronic communication) to any person other than~~
2 ~~a governmental entity.~~

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

9 ~~(A) Presented with a search warrant,~~

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

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

15 ~~(D) Presented with an administrative subpoena~~
16 ~~authorized by statute, an attorney general~~
17 ~~subpoena, or a grand jury or trial subpoena,~~
18 ~~which seeks the disclosure of information~~
19 ~~concerning electronic communication, including~~
20 ~~but not limited to the name, address, local and~~
21 ~~long distance telephone billing records,~~



1 ~~telephone number or other subscriber number or~~
2 ~~identity, and length of service of a subscriber~~
3 ~~to or customer of the service, and the types of~~
4 ~~services the subscriber or customer utilized.~~

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

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

18 (b) Unless otherwise authorized by the court, a
19 governmental entity receiving records or information under this
20 section shall provide notice to the subscriber, customer, or
21 user of the service.



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

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

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

17 1. By amending subsection (a) to read

18 "(a) A governmental entity may include in its ~~[court~~
19 ~~order]~~ search warrant a requirement that the service provider
20 create a backup copy of the contents of the electronic
21 communication without notifying the subscriber or customer. The



1 service provider shall create the backup copy as soon as
2 practicable, consistent with its regular business practices, and
3 shall confirm to the governmental entity that the backup copy
4 has been made. The backup copy shall be created within two
5 business days after receipt by the service provider of the
6 ~~[subpoena or court order.]~~ search warrant."

7 2. By amending subsection (e) to read:

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

- 17 (1) Stating that the applicant is a customer or subscriber
18 to the service from which the contents of electronic
19 communications are sought; and
20 (2) Setting forth the applicant's reasons for believing
21 that the records sought does not constitute probable



1 cause or there has not been substantial compliance
2 with some aspect of the provisions of this part."

3 3. By amending subsection (g) to read:

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

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

21 1. By amending subsection (a) to read:



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

8 2. By amending subsection (c) to read:

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

14 3. By amending subsection (e) to read:

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



1 other person of the existence of the search warrant [~~or court~~
2 ~~order~~] for such period as the court deems appropriate not to
3 exceed ninety days [-] or, at the discretion of the court, no
4 later than the deadline to provide discovery in a criminal case.

5 The court shall enter the order if it determines that there is
6 reason to believe that notification of the existence of the
7 search warrant [~~or court order~~] will result in:

- 8 (1) Endangering the life or physical safety of an
- 9 individual;
- 10 (2) Flight from prosecution;
- 11 (3) Destruction of or tampering with evidence;
- 12 (4) Intimidation of potential witnesses; or
- 13 (5) Otherwise seriously jeopardizing an investigation or
- 14 unduly delaying a trial."

15 PART V

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

18 **"§711-1110.9 Violation of privacy in the first degree.**

19 (1) A person commits the offense of violation of privacy in the
20 first degree if, except in the execution of a public duty or as
21 authorized by law:



- 1 (a) The person intentionally or knowingly installs or
2 uses, or both, in any private place, without consent
3 of the person or persons entitled to privacy therein,
4 any device for observing, recording, amplifying, or
5 broadcasting another person in a stage of undress or
6 sexual activity in that place; ~~[ex]~~
- 7 (b) The person knowingly discloses or threatens to
8 disclose an image or video of another identifiable
9 person either in the nude, as defined in section
10 712-1210, or engaging in sexual conduct, as defined in
11 section 712-1210, without the consent of the depicted
12 person, with intent to harm substantially the depicted
13 person with respect to that person's health, safety,
14 business, calling, career, education, financial
15 condition, reputation, or personal relationships or as
16 an act of revenge or retribution; ~~[provided that:]~~ or
- 17 (c) The person intentionally creates or discloses, or
18 threatens to disclose, an image or video of a
19 fictitious person depicted in the nude, as defined in
20 section 712-1210, or engaged in sexual conduct, as
21 defined in section 712-1210, that includes the



1 recognizable physical characteristics of a known
 2 person so that the image or video appears to depict
 3 the known person and not a fictitious person, with
 4 intent to substantially harm the depicted person with
 5 respect to that person's health, safety, business,
 6 calling, career, education, financial condition,
 7 reputation, or personal relationships, or as an act or
 8 revenge or retribution.

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

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

14 ~~[(B)]~~ (b) Pursuant to a voluntary commercial
 15 transaction ~~[, and]~~ .

16 ~~[(ii)]~~ (3) Nothing in this ~~[paragraph]~~ section shall
 17 be construed to impose liability on a provider of "electronic
 18 communication service" or "remote computing service" as those
 19 terms are defined in section 803-41, for an image or video
 20 disclosed through the electronic communication service or remote
 21 computing service by another person.



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.

