



Information Privacy and Security Council

Meeting Agenda

March 18, 2020

1:00 p.m.

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

- I. Call to Order
- II. Review and Approval of the December 18, 2019 Meeting Minutes
- III. Public Testimony on Agenda Items

Interested persons may submit testimony on any agenda item in writing submitted in advance to Information Privacy and Security Council (IPSC), 1151 Punchbowl St., Room B-10, Honolulu, HI 96813; or email ETS@hawaii.gov, Subject: IPSC Testimony. Each individual or representative of an organization is allotted three minutes for testimony.

- IV. House Bill 2572 H.D.2, Relating to Privacy, Discussion and Appropriate Action
https://www.capitol.hawaii.gov/session2020/bills/HB2572_HD2_.htm

- V. 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.

- VI. Good of the Order
 - a) Announcements
 - b) Next meeting: April 15, 2020

- VII. Adjournment

Individuals who require special needs accommodation are invited to call (808) 586-6000 at least three working days in advance of the meeting.



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.

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, Senate Draft 1 (2019), established the

4

twenty-first century privacy law task force, whose membership

5

consisted of individuals in government and the private sector

6

with an interest or expertise in privacy law in the digital era.

7

The resolution found that public use of the internet and related

8

technologies has significantly expanded in recent years, and

9

that a lack of meaningful government regulation has resulted in

10

personal privacy being compromised. Accordingly, the

11

legislature requested that the task force examine and make

12

recommendations regarding existing privacy laws and regulations

13

to protect the privacy interests of the people of Hawaii.

14

The legislature further finds that the task force

15

considered a spectrum of related privacy issues which have been

16

raised in Hawaii and other states in recent years. Numerous

17

states have begun to address the heightened and unique privacy



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

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

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



1 and expanded to include various personal identifiers and data
2 elements that are found in more comprehensive laws.

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

11 The task force also recommended that explicit consent be
12 required before an individual's internet browser history and
13 content accessed may be shared or sold to a third party.

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

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



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

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

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

PART II

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

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

18 "Identifier" means a common piece of information related
 19 specifically to an individual, that is commonly used to identify
 20 that individual across technology platforms, including a first

1 name or initial, and last name; a user name for an online
2 account; a phone number; or an email address.

3 "Specified data element" means any of the following:

- 4 (1) An individual's social security number, either in its
5 entirety or the last four or more digits;
6 (2) Driver's license number, federal or state
7 identification card number, or passport number;
8 (3) A federal individual taxpayer identification number;
9 (4) An individual's financial account number or credit or
10 debit card number;
11 (5) A security code, access code, personal identification
12 number, or password that would allow access to an
13 individual's account;
14 (6) Health insurance policy number, subscriber
15 identification number, or any other unique number used
16 by a health insurer to identify a person;
17 (7) Medical history, medical treatment by a health care
18 professional, diagnosis of mental or physical
19 condition by a health care professional, or
20 deoxyribonucleic acid profile;



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

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

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

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

- 14 ~~(1) Social security number;~~
- 15 ~~(2) Driver's license number or Hawaii identification card~~
 16 ~~number; or~~
- 17 ~~(3) Account number, credit or debit card number, access~~
 18 ~~code, or password that would permit access to an~~
 19 ~~individual's financial account.]~~

20 identifier in combination with one or more specified data
 21 elements, when the specified data element or elements are not

1 encrypted. "Personal information" [~~does~~] shall not include
2 publicly available information that is lawfully made available
3 to the general public from federal, state, or local government
4 records."

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

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

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

20 (2) Any health plan or healthcare provider and its
21 business associates that [~~is~~] are subject to and in



1 compliance with the standards for privacy or
 2 individually identifiable health information and the
 3 security standards for the protection of electronic
 4 health information of the Health Insurance Portability
 5 and Accountability Act of 1996."

6 PART III

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

10 "§481B- Sale of geolocation information without consent
 11 is prohibited. (a) No person, in any manner, or by any means,
 12 shall sell or offer for sale geolocation information that is
 13 recorded or collected through any means by mobile devices or
 14 location-based applications without the explicit consent of the
 15 individual who is the primary user of the device or application.

16 (b) As used in this section:

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

19 "Emergency" means the imminent or actual occurrence of an
 20 event, which has the likelihood of causing extensive injury,
 21 death, or property damage.



1 "Geolocation information" means information that is:

2 (1) Not the contents of a communication;

3 (2) Generated by or derived from, in whole or in part, the

4 operation of a mobile device, including but not

5 limited to a smart phone, tablet, fitness tracker,

6 e-reader, or laptop computer; and

7 (3) Sufficient to determine or infer the precise location

8 of the user of the device.

9 "Location-based application" means a software application

10 that is downloaded or installed onto a device or accessed via a

11 web browser and collects, uses, or stores geolocation

12 information.

13 "Precise location" means any data that locates a user

14 within a geographic area that is equal to or less than the area

15 of a circle with a radius of one mile.

16 "Sale" means selling, renting, releasing, disclosing,

17 disseminating, making available, transferring, or otherwise

18 communicating orally, in writing, or by electronic or other

19 means, a user's geolocation information to another business or a

20 third party for monetary or other valuable consideration.

21 "Sale" shall not include the releasing, disclosing,



1 disseminating, making available, transferring, or otherwise
2 communicating orally, in writing, or by electronic or other
3 means, a user's geolocation information for the purpose of
4 responding to an emergency.

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

7 §481B- Sale of internet browser information without
8 consent is prohibited. (a) No person, in any manner, or by any
9 means, shall sell or offer for sale internet browser information
10 without the explicit consent of the subscriber of the internet
11 service.

12 (b) As used in this section:

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

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

- 17 (1) Web browsing history;
18 (2) Application usage history;
19 (3) The origin and destination internet protocol
20 addresses;



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

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

6 "Internet service" means a retail service that provides the
7 capability to transmit data to and receive data through the
8 Internet using a dial-up service, a digital subscriber line,
9 cable modem, fiber optics, wireless radio, satellite, powerline,
10 or other technology used for a similar purpose.

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

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



1 PART IV

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

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

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

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



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

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

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

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

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

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



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

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

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

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

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

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



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

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

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

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



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

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

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

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

19 1. By amending subsection (a) to read

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



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

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

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

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



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

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

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

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



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

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

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

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

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

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



1 search warrant, or court order is directed, not to notify any
2 other person of the existence of the search warrant [~~7~~ ~~or court~~
3 ~~order~~] for such period as the court deems appropriate not to
4 exceed ninety days [~~7~~] or, at the discretion of the court, no
5 later than the deadline to provide discovery in a criminal case.

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

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

16 PART V

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

19 "§711-1110.9 Violation of privacy in the first degree.

- 20 (1) A person commits the offense of violation of privacy in the



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

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

9 (b) The person knowingly discloses or threatens to
10 disclose an image or video of another identifiable
11 person either in the nude, as defined in section 712-
12 1210, or engaging in sexual conduct, as defined in
13 section 712-1210, without the consent of the depicted
14 person, with intent to harm substantially the depicted
15 person with respect to that person's health, safety,
16 business, calling, career, education, financial
17 condition, reputation, or personal relationships or as
18 an act of revenge or retribution; [~~provided that~~] or

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



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

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

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

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

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



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

3 ~~[(2)]~~ (4) Violation of privacy in the first degree is a
4 class C felony. In addition to any penalties the court may
5 impose, the court may order the destruction of any recording
6 made in violation of this section.

7 ~~[(3)]~~ (5) Any recording or image made or disclosed in
8 violation of this section and not destroyed pursuant to
9 subsection ~~[(2)]~~ (4) shall be sealed and remain confidential."

10

PART VI

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

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

16 SECTION 12. This Act shall take effect on July 1, 2050.



Report Title:

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

Description:

Modernizes "personal information" for the purposes of 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. Effective 7/1/2050. (HD2)

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

