Senior Deputy Prosecuting Attorney Chris Van Mater:

The attached proposal suggests amendments to Hawaii's version of the federal Stored Communications Act, which can be found at Hawaii Revised Statutes (HRS) Sections 803-47.6 through 803-47.8. There is also a proposal to amend HRS Section 803-41, which is the definition section that governs Sections 803-47.6 through 803-47.8.

Regarding the proposed amendments to HRS Section 803-47.6, that section governs law enforcement's legal authority to compel disclosure of various forms of information stored by "electronic communication services" (such as Google, Apple, Microsoft, Verizon, Hawaiian Telcom, Spectrum, Facebook, and others) and "remote computing services" (such as web hosting companies and cloud-based storage providers like Dropbox). Currently, if law enforcement wants to compel disclosure of the "contents" of communications (such as e-mail, text messages, or private "comments or tweets"), law enforcement must obtain a search warrant. If law enforcement wants to compel disclosure of "transactional records" (such as IP logs, cell site data, and e-mail headers), law enforcement must obtain a court order. If law enforcement wants to compel disclosure of call detail records, or subscriber or account user information, law enforcement is permitted to use a subpoena. The attached proposal eliminates the disparate treatment between "content", "transactional records", and account user records, and treats all forms of electronically stored data the same, namely they receive the same protection against disclosure. Thus, if the proposal is adopted, law enforcement would be required to obtain a search warrant (from a neutral judge) before accessing any form of electronically stored data from "electronic communication services" and "remote computing services", or obtain the consent of the subscriber, customer, or user of the service. Note: "Electronically stored data" is defined in the proposal relating to HRS Section 803-41.

Regarding the proposed amendments to HRS Section 803-47.7, that section relates to "court orders" granted at the request of law enforcement that order "electronic communication services" and "remote computing services" to make a "backup" of an online account. Since the proposal to HRS Section 803-47.6 will require that law enforcement obtain a "search warrant" (instead of a "court order"), the proposal to HRS Section 803-47.7 simply replaces the "court order" language with the "search warrant" language.

Regarding the proposed amendments to HRS Section 803-47.8, that section relates to scenarios when the court can delay disclosure to a user. In practice, the court grants delayed disclosure in close to 100% of the cases involving law enforcement's access to online data. Court-approved non-disclosure orders are based on the need to prevent the harms that are set forth in HRS Section 803-47.8(e). In practice, law enforcement discloses their access to records as part of the discovery process in criminal cases. The discovery materials, including copies of the legal process and records obtained, are provided in discovery to defense counsel and the defendant within 10 days of arraignment, pursuant to Rule 16 of the Hawaii Rules of Penal Procedure (HRPP). The proposal to HRS Section 803-47.8 would retain the judicial discretion provision, and require that disclosure be made no later than the deadline for providing discovery in a criminal case.

Report Title:

Description:

THIRTY-FIRST LEGISLATURE, 2020
STATE OF HAWAII

___. B. NO.

A BILL FOR AN ACT

RELATING TO_____.

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

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

§803-41 Definitions. As used in this part, unless the context clearly requires otherwise:

"Aggrieved person" means a person who was party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed.

"Aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception.

"Bait vehicle" means any vehicle used by law enforcement to further an investigation of and deter unauthorized entry into a motor vehicle or unauthorized control of propelled vehicles.

"Communication common carrier" means any person engaged as a common carrier for hire in interstate or foreign communication by wire or radio or in intrastate, interstate, or foreign radio

transmission of energy, except where reference is made to communication common carriers not subject to this part; provided that a person engaged in radio broadcasting, to the extent the person is so engaged, shall not be deemed a communication common carrier.

"Contents" when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.

"Designated judge" means a circuit court judge designated by the chief justice of the Hawaii supreme court to issue orders under this part.

"Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system that affects intrastate, interstate, or foreign commerce. The term "electronic communication" includes, but is not limited to, "display pagers" which can display [a] visual message as part of the paging process, but does not include:

(1) Any wire or oral communication;

(2) Any communication made through a tone-only paging device;

(3) Any communication from a tracking device; or

(4) Electronic funds transfer information stored by [a] financial institution in a communications system used for the electronic storage and transfer of funds.

"Electronic communication service" means any service that provides to users thereof the ability to send or receive wire or electronic communications.

"Electronic communication system" means any wire, radio, electromagnetic, photo-optical, or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of these communications.

"Electronic, mechanical, or other device" means any device or apparatus that can be used to intercept a wire, oral, or electronic communication other than:

(1) Any telephone or telegraph instrument, equipment, or facility, or any component thereof[:]

(A) Furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by the

subscriber or user for connection to the facilities of the services and used in the ordinary course of its business; or

(B) Being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of the officer's duties; or

(2) A hearing aid or similar device being used to correct subnormal hearing to a level not better than average.

"Electronic storage" means:

(1) Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(2) Any storage of the communication by an electronic communication service for purposes of backup protection of the communication.

"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, and includes, but is not limited to, 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.

"Intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

"Investigative or law enforcement officer" means any officer of the State or political subdivision thereof, who is empowered by the law of this State to conduct investigations of or to make arrests for offenses enumerated in this part.

"Oral communication" means any utterance by a person exhibiting an expectation that the utterance is not subject to interception under circumstances justifying that expectation, but the term does not include any electronic communication.

"Organized crime" means any combination or conspiracy to engage in criminal activity.

"Pen register" means a device that records or decodes electronic or other impulses that identify the numbers dialed or otherwise transmitted on the telephone line or cellular network to which the device is connected, or that identifies the numbers that a device uses to connect to a wire or electronic communications service, but the term does not include any device used by a provider or customer of a wire or electronic

communication service for billing, or recording as an incident to billing, for communication services provided by the provider or any device used by a provider or customer of a wire communication service for cost accounting or other similar purposes in the ordinary course of its business.

"Person" means any official, employee, or agent of the United States or this State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.

"Readily accessible to the general public" means, with respect to radio communication, that the communication is not:

(1) Scrambled or encrypted;

(2) Transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of the communication;

(3) Carried on a subcarrier or other signal subsidiary to a radio transmission;

(4) Transmitted over a communication system provided by a common carrier, unless the communication is a tone-only paging system communication; or

(5) Transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the

Federal Communications Commission, unless in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio.

"Remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communication system.

"Tracking device" means an electronic or mechanical device that permits the tracking of the movement of a person or object, but does not include a device when installed:

(1) In a motor vehicle or other vehicle by or with the permission of the owner or person in lawful possession of the motor vehicle or other vehicle for the purpose of tracking the movement of the motor vehicle or other vehicle; or

(2) By or at the request of a police department or law enforcement agency in a "bait vehicle".

"Trap and trace device" means a device that captures the incoming electronic or other impulses that identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.

"User" means any person or entity that:

(1) Uses an electronic communication service; and

(2) Is duly authorized by the provider of the service to engage in such use.

"Wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of intrastate, interstate, or foreign communications. The term "wire communication" includes, but is not limited to, cellular telephones, cordless telephones, "tone and voice" pagers which transmit a voice message along with a paging signal, and any electronic storage of a wire communication.

SECTION 2. Chapter 803, Hawaii Revised Statutes, is amended to read as follows:

§803-47.6 Requirements for governmental access. (a) Except as otherwise provided by law, a [~~A~~] governmental entity may require [~~the disclosure by~~] a provider of an electronic communication service and a provider of a remote computing service to disclose electronically stored data [~~of the contents~~

~~of an electronic communication~~]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)~~ (b) Unless otherwise authorized by the court, [~~A~~] a governmental entity receiving records or information under this [~~subsection~~]section is [~~not~~]required to provide notice to [~~a~~]the subscriber, [~~or~~]customer, or user of the service.

~~[(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.~~]

[~~(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 3. Chapter 803, Hawaii Revised Statutes, is amended to read as follows:

§803-47.7 Backup preservation. (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.

(b) The governmental entity must give notice to the subscriber or customer within three days of receiving confirmation that a backup record has been made, unless notice is delayed pursuant to the procedures herein.

(c) The service provider shall not destroy the backup copy until the later of:

(1) The delivery of the information; or

(2) The resolution of any proceedings, including any appeal therefrom, concerning a court order.

(d) The service provider shall release the backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer, if the service provider:

(1) Has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

(2) Has not initiated proceedings to challenge the request of the governmental entity.

(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.

(f) Upon receiving a copy of the motion from the subscriber or customer, the governmental agency shall file a sworn response to the court to which the motion is assigned. The response shall be filed within fourteen days. The response may ask the court for an in camera review, but must state reasons justifying such a review. If the court is unable to rule solely on the motion or application and response submitted, the court may conduct such additional proceedings as it deems appropriate. A ruling shall be made as soon as practicable after the filing of the governmental entity's response.

(g) If the court finds that the applicant is not the subscriber or customer whose communications are sought, or that there is reason to believe that the law enforcement inquiry is

legitimate and the justification for the communications sought is supported by probable cause, the application or motion shall be denied, and the court shall order the release of the backup copy to the government entity. A court order denying a motion or application shall not be deemed a final order, and no interlocutory appeal may be taken therefrom by the customer. If the court finds that the applicant is a proper subscriber or customer and the justification for the communication sought is not supported by probable cause or that there has not been substantial compliance with the provisions of this part, it shall order vacation of the [~~order~~] warrant previously issued.

SECTION 4. Chapter 803, Hawaii Revised Statutes, is amended to read as follows:

§803-47.8 Delay of notification. (a) A governmental entity may as part of a request for a [~~court order~~] search warrant include a provision that notification be delayed for a period not exceeding ninety days or, at the discretion of the court, no later than the deadline to provide discovery in a criminal case, if the court determines that notification of the existence of the court order may have an adverse result.

(b) An adverse result for the purpose of subsection (a) of this section is:

(1) Endangering the life or physical safety of an individual;

(2) Flight from prosecution;

(3) Destruction of or tampering with evidence;

(4) Intimidation of a potential witness; or

(5) Otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(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.

(d) Upon expiration of the period of delay of notification, the governmental entity shall serve upon, or deliver by registered mail to, the customer or subscriber a copy of the process or request together with notice that:

(1) States with reasonable specificity the nature of the law enforcement inquiry; and

(2) Informs the customer or subscriber:

(A) Information maintained for the customer or subscriber by the service provider or request was supplied to or

requested by that governmental authority and the date on which the supplying or request took place;

(B) Notification of the customer or subscriber was delayed;

(C) The governmental entity or court that made the certification or determination upon which the delay was made; and

(D) The provision of this part that allowed the delay.

(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.

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 approval.

INTRODUCED BY: _____

State Comprehensive-Privacy Law Comparison

The 16 common privacy provisions include the following:

- **The right of access to personal information collected** — The right for a consumer to access from a business/data controller the information collected or categories of information collected about the consumer; right may only exist if a business sells information to a third party.
    - California. Ratified as part of CCPA and effective Jan. 1, 2020. Allows customers to request specifics about their data.

      A business that collect data must provide: 1) the categories of personal information the business has collected about the consumer; 2) the specific pieces of personal information the business has collected; 3) the categories of sources from which the personal information was collected; 4) the business or commercial purpose for the collection; and 5) the categories of third parties with whom the business shares the personal information.

      A businesses that sell data also provide 1) the categories of personal information it has collected about the consumer; 2) the categories of personal information it has sold about the consumer; 3) the categories of third parties to whom the personal information was sold (organized by category of personal information for each third party); and 4) the categories of personal information it disclosed about the consumer for a business purpose.
    - GDPR. Data controllers must provide detailed information about its personal data collection and data processing activities. The notice must include specific information depending on whether the data is collected directly from the data subject or a third party
- **The right of access to personal information shared with a third party** — The right for a consumer to access personal information shared with third parties.
    - California. Ratified as part of CCPA and effective Jan. 1, 2020. Consumers have a right to request receive details regarding any third parties with which it shares information.
- **The right to rectification** — The right for a consumer to request that incorrect or outdated personal information be corrected but not deleted.
    - GDPR grants data subjects the right to 1) correct inaccurate personal data and 2) complete incomplete personal data.
- **The right to deletion** — The right for a consumer to request deletion of personal information about the consumer under certain conditions.
    - California. Ratified as part of CCPA and effective Jan. 1, 2020. A consumer has the right to deletion of personal information a business has collected, subject to the following exceptions: when data is required to complete a customer-initiated transaction, to detect/protect/prosecute security incidents, to identify errors, support free speech, research in the public interest, expected internal uses, legal compliance, and other internal uses. The business must also instruct its service providers to delete the data.
    - US federal law: The Children's Online Privacy Protection Act (COPPA) applies to minors under the age of 13 and requires that data be deleted when it is no longer "reasonably necessary to fulfill the purpose for which the information was collected."

- GDPR. Data subjects have the right to request erasure of personal data under six circumstances with nine exceptions. Data controllers must also take reasonable steps to inform any other data controllers also processing the data.
  https://www.i-scoop.eu/gdpr/right-erasure-right-forgotten-gdpr/

- **The right to restriction of processing** — The right for a consumer to restrict a business' ability to process personal information about the consumer.

  - GDPR grants data subjects the right to object to processing for profiling, direct marketing, and statistical, scientific, or historical research purposes.

- **The right to data portability** — The right for a consumer to request personal information about the consumer be disclosed in a common file format.

  - California. Ratified as part of CCPA and effective Jan. 1, 2020. A business must provide personal information in a readily useable format to enable a consumer to transmit the information from one entity to another entity without hindrance.

  - GDPR includes a new right to data portability to 1) receive a copy of the personal data in a structured, commonly used and machine-readable format, and 2) transmit the personal data to another data controller (including directly by another data controller where possible).

- **The right to opt out of the sale of personal information**— The right for a consumer to opt out of the sale of personal information about the consumer to third parties.

  - California is opt-out for adults and opt-in minors under the age of 16; consent by minor if over 13, by parent otherwise. Ratified as part of CCPA and effective Jan. 1, 2020.
  - Maine is opt-in for sale. Only covers Internet Service Providers.
  - Nevada is opt-out. Covers any operator of a website.

- **The right against solely automated decision making** — A prohibition against a business making decisions about a consumer based solely on an automated process without human input.

  - GDPR. Data subjects have the right to not be subject to *solely* automated decision making, including profiling, which has legal or other significant effects on the data subject, subject to three exceptions (necessary for a contract, authorized by law, or based on explicit consent).

- **A consumer private right of action** — The right for a consumer to seek civil damages from a business for violations of a statute.

  US state level: Limited to data breach notification:
  - Alaska. For failure to notify. Under unfair and deceptive trade practices. Brought by individual against non-governmental entity and Dept. of Administration against governmental agencies. Actual damages capped at $500.
  - California. $100-$750 or actual damages, whichever is greater. May also include injunctive or declarative relief. Expanded under CCPA. Grants a 30-day cure period. Amendment S.B. 561 to further expand the private right of action to any non-compliance of CCPA died in the Senate Appropriations Committee.
    https://www.pbwt.com/data-security-law-blog/a-closer-look-at-the-ccpas-private-right-of-action-and-statutory-damages/
  - Louisiana. Actual damages.
  - Maryland. Under unfair and deceptive trade practices. Does not require actual damage.
  - Massachusetts. Allowed if AG finds deceptive or unfair trade practices have occurred.
  - New Hampshire. Actual damages.
  - North Carolina. Under unfair and deceptive trade practices. Actual damages.

- South Carolina. Actual damages.
- Tennessee. Actual damages. Requires identity theft to have occurred.
- Virginia. Direct economic damages.
- Washington. Under unfair and deceptive trade practices.

- US federal level: The Telephone Consumer Protection Act (TCPA) establishes a private right of action for non-compliance with automated-dialed or recorded phone calls, faxes and texts.

- GDPR establishes a private right of action for material or non-material damage caused by a data controller or data processors breach of compliance with the GDPR.

- **A strict opt-in for the sale of personal information of a consumer less than a certain age** – A restriction placed on a business to treat consumers under a certain age with an opt-in default for the sale of their personal information.

  - California. Opt-in to sale of data for minors under the age of 16; consent by minor if over 13, by parent under 13. Ratified as part of CCPA and effective Jan. 1, 2020.

  - US federal law: The Children's Online Privacy Protection Act (COPPA) requires parental consent for the collection of any data from minors under the age of 13.

- **Notice/transparency requirements** – An obligation placed on a business to provide notice to consumers about certain data practices, privacy operations, and/or privacy programs.

  - California. California Online Privacy Protection Act (CalOPPA), passed in 2004, requires all websites and mobile apps to have a privacy policy. CalOPPA applies to more companies than CCPA. CCPA also requires notice at or before the time of data collection.

  - Maine. Requires notice for ISPs.

  - Nevada. Requires a notice from all operators of websites.

  - US federal law – Graham Leach Bliley requires financial institutions to provide an annual privacy notice. HIPAA requires individual's acknowledgement of privacy notice from covered entities with Protected Health Information.

  - GDPR. Notice must be given at the time of data collection. Children must receive an age appropriate privacy notice.

- **Data breach notification** – An obligation placed on a business to notify consumers and/or enforcement authorities about a privacy or security breach.

  - All 50 states have data breach notification laws.

  - HRS 487-N. recommended updates, including definition of Personal Information.

- **Mandated risk assessment** – An obligation placed on a business to conduct formal risk assessments of privacy and/or security projects or procedures.

  - US federal law – Federal agencies are required by the E-Government Act of 2002 to perform Privacy Impact Assessments (PIAs), an analysis of how personally identifiable information is collected, used, shared, and maintained. The purpose of a PIA is to demonstrate that program managers and system owners at the FTC have consciously incorporated privacy protections throughout the development life cycle of a system or program.

- GDPR. In the event a project results in a high risk to the rights and freedoms of data subjects, the GDPR requires a Data Protection Impact Assessment (DPIA).

- **A prohibition on discrimination against a consumer for exercising a right** — A prohibition against a business treating a consumer who exercises a consumer right differently than a consumer who does not exercise a right.

    - California. Ratified as part of CCPA and effective Jan. 1, 2020. A business must not discriminate against a consumer because they exercised their rights. However, a business may charge differently if that difference reasonably relates to the value provided by the consumer's data. Businesses may also offer financial incentives if they are disclosed in terms or online privacy policy, and require opt-in consent.

    - Maine. ISPs may not refuse service or charge a penalty for refusal to provide consent.

    - Implicit in GDPR.

- **A purpose limitation** — An EU General Data Protection Regulation–style restrictive structure that prohibits the collection of personal information except for a specific purpose.

    - GDPR requires that data can only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is allowed. (Article 5)

- **A processing limitation** — A GDPR-style restrictive structure that prohibits the processing of personal information except for a specific purpose.

    - GDPR. Processing of personal data is only lawful if and to the extent that at least one of the following six principles applies: 1) consent by the data subject, 2) required for a contract, 3) to comply with a legal obligation, 4) necessary to protect the vital interest of a natural person, 5) in the public interest of under official authority, and 6)processing is necessary for the purposes of the legitimate interests, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual which require protection of personal data, in particular where the data subject is a child.

https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/

Hawaii (HRS 487-N) Current

"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.

Proposed

"Personal information" means an Identifier in combination with one or more Specified Data Elements.

(i) An Identifier is a common piece of information related specifically to the individual, which is used to identify that individual, such as first name/initial and last name, a user name for an online account, a phone number, or email address.

(ii) "Specified Data Element" means any of the following:

(a) An individual's social security number, either in its entirety or the last four digits.

(b) Driver's license number, federal or state identification card number, or passport number.

(c) An individual's federal or State of Hawaii taxpayer identification number.

(d) An individual's financial account number or credit or debit card number.

(e) A security code, access code, PIN, or password that would allow access to an individual's account.

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

(g) Medical history, medical treatment by a health-care professional, diagnosis of mental or physical condition by a health care professional, or deoxyribonucleic acid profile.

(h) 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.

(i) A digital signature or private key that is unique to an individual and that is used to authenticate or sign an electronic record.

Arizona

"Personal information":

(a) Means any of the following:

(i) An individual's first name or first initial and last name in combination with one or more specified data elements.

(ii) An individual's user name or e-mail address, in combination with a password or security question and answer, that allows access to an online account.

"Specified data element" means any of the following:
(a) An individual's social security number.
(b) The number on an individual's driver license issued pursuant to
Section 28-3166 or nonoperating identification license issued pursuant to section 28-3165.
(c) A private key that is unique to an individual and that is used to authenticate or sign an electronic record.
(d) An individual's financial account number or credit or debit card number in combination with any required security code, access code or password that would allow access to the individual's financial account.
(e) An individual's health insurance identification number.
(f) Information about an individual's medical or mental health treatment or diagnosis by a health care professional.
(g) An individual's passport number.
(h) An individual's taxpayer identification number or an identity protection personal identification number issued by the United States internal revenue service.
(i) Unique biometric data generated from a measurement or analysis of human body characteristics to authenticate an individual when the individual accesses an online account.

California

"Personal information" means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.

NOTE: Definition includes information or data collected through the use or operation of an automated license plate recognition system.
Definition also captures a user name or email address in combination with a password or security question and answer that would permit access to an online account.

Delaware

Personal information'' means a Delaware resident's first name or first initial and last name in combination with any 1 or more of the following data elements that relate to that individual:
1. Social Security number.
2. Driver's license number or state or federal identification card number.
3. Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.
4. Passport number.
5. A username or email address, in combination with a password or security question and answer that would permit access to an online account.
6. Medical history, medical treatment by a health-care professional, diagnosis of mental or physical condition by a health care professional, or deoxyribonucleic acid profile.

7. Health insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person.
8. Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes.
9. An individual taxpayer identification number.

Illinois

"Personal information" means either of the following:

(1) 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 or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security:

(A) Social Security number.

(B) Driver's license number or State identification card number.

(C) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

(2) User name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.

Louisiana

(4)(a) "Personal information" means the first name or first initial and last name of an individual resident of this state in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted:

(i) Social security number.

(ii) Driver's license number or state identification card number.

(iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(iv) Passport number.

(v) Biometric data. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as fingerprints, voice print, eye retina or iris, or other unique biological characteristic that is used by the owner or licensee to uniquely authenticate an individual's identity when the individual accesses a system or account.

New York

(a) "Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;

(b) "Private information" shall mean personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired:

(1) social security number;

(2) driver's license number or non-driver identification card number;

or

(3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;

North Carolina

The term "identifying information" as used in this Article includes the following:

(1) Social security or employer taxpayer identification numbers.
(2) Driver's license, State identification card, or passport numbers.
(3) Checking account numbers.
(4) Savings account numbers.
(5) Credit card numbers.
(6) Debit card numbers.
(7) Personal Identification (PIN) Code as defined in G.S. 14-113.8(6).
(8) Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names.
(9) Digital signatures.
(10) Any other numbers or information that can be used to access a person's financial resources.
(11) Biometric data.
(12) Fingerprints.
(13) Passwords.
(14) Parent's legal surname prior to marriage.

North Dakota

"Personal information" means an individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted:

(1) The individual's social security number;
(2) The operator's license number assigned to an individual by the department of transportation under section 39-06-14;
(3) A nondriver color photo identification card number assigned to the individual by the department of transportation under section 39-06-03.1;
(4) The individual's financial institution account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts;
(5) The individual's date of birth;
(6) The maiden name of the individual's mother;

(7) Medical information;
(8) Health insurance information;
(9) An identification number assigned to the individual by the individual's employer in combination with any required security code, access code, or password; or
(10) The individual's digitized or other electronic signature.

Oregon

"Personal information" means:

(a) A consumer's first name or first initial and last name in combination with any one or more of the following data elements, if encryption, redaction or other methods have not rendered the data elements unusable or if the data elements are encrypted and the encryption key has been acquired:

(A) A consumer's Social Security number;

(B) A consumer's driver license number or state identification card number issued by the Department of Transportation;

(C) A consumer's passport number or other identification number issued by the United States;

(D) A consumer's financial account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account;

(E) Data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction;

(F) A consumer's health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; or

(G) Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer.

Wisconsin

"Personal information" means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable:

1. The individual's social security number.
2. The individual's driver's license number or state identification number.
3. The number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account.
4. The individual's deoxyribonucleic acid profile, as defined in s. 939.74 (2d) (a).
5. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

Wyoming

"Personal identifying information" means the first name or first initial and last name of a person in combination with one (1) or more of the data elements specified in W.S. 6-3-901(b)(iii) through (xiv).

W.S. 6-3-901(b):
As used in this section "personal identifying information" means the name or any of the following data elements of an individual person:
(i) Address;
(ii) Telephone number;
(iii) Social security number;
(iv) Driver's license number;
(v) Account number, credit card number or debit card number in combination with any security code, access code or password that would allow access to a financial account of the person;
(vi) Tribal identification card;
(vii) Federal or state government issued identification card;
(viii) Shared secrets or security tokens that are known to be used for data based authentication;
(ix) A username or email address, in combination with a password or security question and answer that would permit access to an online account;
(x) A birth or marriage certificate;
(xi) Medical information, meaning a person s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;
(xii) Health insurance information, meaning a person s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the person or information related to a person s application and claims history;
(xiii) Unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes;
(xiv) An individual taxpayer identification number.

From Jael Makagon, Santa Clara County Privacy Office

- Privacy related to information held by Internet Service Providers (ISPs)
    - ISPs are in a unique position. The average customer must use an ISP to access the internet, and as a result ISPs can see every web address and – depending on the level of security offered by the website – even the page content of every website that their customers visit. In 2017, US Congressional Republicans blocked the FCC from regulating ISPs's use of personal information, so many states have sought to fill that gap with state legislation. Currently, Maine, Minnesota, and Nevada have laws that require confidentiality of ISP customer information, and many other states are considering similar legislation.
    - I realize a similar bill (H.B. 2296) failed in the HI leg last year, so there may be some specific context that prevents this from being a viable option.

- Regulation of data brokers
    - There is widespread agreement that data brokers are a problematic industry, and the Federal Trade Commission has called on Congress to pass legislation that would establish a nationwide registry of data brokers. Vermont passed a law in 2018 requiring data brokers to register with the state, and California's version is awaiting the governor's signature (I don't think California's version is the best way, because they make it very easy to develop a "business relationship" with a data broker who then would be exempt from the law). But this is an area where states are leading and where I think there would be public support if Hawaii wanted to pass its own version.

- Privacy principles for the State
    - My job at the County of Santa Clara is to operationalize privacy in a variety of ways, from privacy impact assessments of County systems, to privacy reviews of software, to helping departments draft surveillance use policies for their surveillance technology. I think my job would be easier if the County had a set of privacy principles, like Seattle's that I could refer to as a guidepost when asking departments to change their behavior to be more privacy protective. This might take the form of a resolution, but it would be helpful to chart a course for future privacy efforts if the State developed some core principles on the topic.

- Surveillance technology oversight
    - My personal goal for Hawaii is to require government departments that want to use surveillance technology, such as automated license plate readers, video cameras, etc., to create policies that govern the use of that technology. These kinds of requirements are generally being created at the City and County level, which makes sense because those are the localities that typically control law enforcement agencies such as the police and sheriff. I'm not sure if there's a place for the State to be involved, but it may be an area the Task Force wants to consider depending on the current dynamic in Hawaii.

From SAG-AFTRA

This legislation will provide victims of nonconsensual, digitally produced sexually explicit material, such as Deepfakes pornography, a civil cause of action to sue bad actors in open court for economic, reputational, and emotional harm. New technologies allow content creators to manipulate images to depict individuals as engaging in sexual activity or as performing in the nude without their consent or participation.

As reported by the Washington Post and other news outlets, individuals (mostly women) are being harassed or exploited online with these videos. Internet users can use a publicly available artificial intelligence algorithm to transform still images of a person into live action performance by realistically inserting their face onto the body of a porn performer.

SAG-AFTRA's concerns do not stop at unauthorized pornography on the internet. Filmmakers can also use this technology in mainstream content to depict a SAG-AFTRA member as performing in the nude or as engaging in sexual activity without meaningful consent. This form of digital doubling can cause enormous harm, even though the audiovisual work does not show the performer's actual intimate body parts. In post-production, filmmakers now have tools to remove underwear, create a digital replica of the individual, or to place the head of a performer on the real body of another. Unfortunately, some performers have suffered at the hands of this technology in film production, and the problem will only intensive as this technology becomes more advanced and freely accessible.

Individuals need a new law that targets this kind of abuse and establishes special rules around consent and remedies, so that victims have civil remedies and bad actors are deterred from making the videos in the first place. As reported by Vice, federal child pornography laws have certainly deterred Deepfakes creators from using photos of children altogether. Proving targeted laws have a deterrence effect.