Summaries of California Privacy Law Changes

Bills signed on Tuesday Oct. 8 and Friday Oct. 11, 2019

Data Breach Notification

Assembly Bill 1130 amends the definition of Personal Information in the data breach notification law to include tax identification numbers, passport numbers, military identification numbers, or other unique identification numbers issued on a government document commonly used to verify the identity of a specific individual.

Data Broker Registration

Assembly Bill 1202 requires data brokers to register with the attorney general, and requires the attorney general to create a publicly available registry of data brokers on its website, and grants the AG enforcement authority for violations of these requirements.

Facial Recognition and Police Body Cams

Assembly Bill 1215 prohibits a law enforcement agency or law enforcement officer from installing, activating, or using any biometric surveillance system in connection with an officer camera or data collected by an officer camera. The bill authorizes a person to bring an action for equitable or declaratory relief against a law enforcement agency or officer who violates that prohibition. The bill repeals these provisions on January 1, 2023.

CCPA

Personal Information Definition

Assembly Bill 874 and Assembly Bill 1355 amend the definition of "personal information" to include "reasonably" in two places to state: "information that identifies, relates to, describes, is ***reasonably*** capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is ***reasonably*** capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household."

Clarifies that "personal information" does not include "consumer information that is de-identified or aggregate consumer information."

Clarifies that "publicly available" in the definition of "personal information" means "information that is lawfully made available from federal, state, or local government records. 'Publicly available' does not mean biometric information collected by a business about a consumer without the consumer's knowledge."

Notice

Consumer Requests Disclosure Methods. Assembly Bill 1564 permits a business that operates exclusively online and has a direct relationship with the consumer to provide only an email

address as the method for submitting consumer requests. All other businesses must have two designated methods (including at least a toll-free number).

Notice Requirement. Assembly Bill 1355 provides that a business's privacy policy must disclose "the categories of personal information it has collected ***about consumers***."

Data Deletion / Sale

Vehicle Information. Assembly Bill 1146 creates a carve-out so that the right of deletion doesn't apply to vehicle repair information, like warranties and recall-related info if the vehicle or ownership information is shared for the purpose of a vehicle repair covered by a vehicle warranty or a recall."

One Year Exemptions

Employee / Job Candidate One-Year Exemption. Assembly Bill 25 creates a one-year exemption for employee data, meaning that the law doesn't apply to personal info collected from workers, job applicants or contractors. The legislature will revisit this issue next year.

Business-to-Business (B2B) One-Year Exemption. Assembly Bill 1355 amends the CCPA until January 1, 2021, to add Cal. Civ. Code § 1798.145(l), which exempts written or verbal communication or a transaction between the business and the consumer, where the consumer is an employee or owner of another company, and whose communications with the business occur solely within the context of the business providing or receiving a product or service to such company. B2B consumers are still entitled to (a) bring a private right of action under the law and (b) to the opt-out of sale right, but the opt-out of sale notice provisions would not apply to businesses.

Possible ballot initiative

The California Privacy Rights And Enforcement Act Of 2020
The CPREA would establish new consumer rights around the use and sale of sensitive personal information, including health, financial, racial and ethnic, as well as precise geolocation information. It would also triple CCPA fines for improper use of children's data, require transparency around automatic decision making and profiling, amend election disclosure laws, and significantly, establish a new enforcement authority in the state.

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.

Data Broker laws

Vermont (H.764)

Defines "Data Broker" as a company that collects and sells/licenses the personal information of a consumer with whom it does not have a direct business relationship.
Requires that data brokers maintain industry standard security practices, register annually with the state ($100 fee), and disclose a data breach.
Also makes it illegal to acquire information from a data broker for fraud, stalking, harassment, or discrimination pertaining to housing or employment. Defines these as deceptive and unfair trade practices.
Eliminates fees for freezing a credit report and charges the Attorney General to propose a method to make credit freezes easier for consumers to manage.
Enforcement is by the state Attorney General with fines up to $10,000 for failure to register.

- ⇨ Over 120 companies have registered. Consumers have been directed to opt-out directly with data brokers and report violations to FTC.

California (AB 1202)

Requires data brokers to register with the Attorney General (AG). Requires AG to create a webpage listing registered data brokers.
Bill refers to CCPA consumer rights of data access and data deletion. It cites that Data Broker registration is necessary so consumers can exercise these rights.

The sale of personal information

- **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.

- **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.

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.

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.

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: _____

HONOLULU POLICE DEPARTMENT

POLICY
AUXILLARY AND TECHNICAL SERVICES

September 14, 2015	Policy Number 8.21

FACIAL RECOGNITION PROGRAM

POLICY

To establish procedures when using the Honolulu Police Department's (HPD) facial recognition program to identify possible suspects or other investigative leads.

PROCEDURE

I. BACKGROUND

A. The facial recognition program was created in conjunction with the Hawaii Criminal Justice Data Center, Department of the Attorney General. The program helps to identify possible suspects by generating investigative leads for detectives.

B. The facial recognition system is a computer program that searches and compares existing photographs or videos to known mug shot photographs. The system is used to link known crimes and persons and provide assistance with identifying a potential suspect(s).

C. The system is designed to compare unknown suspects with new and current photographs that are continually updated to link certain crimes to individuals and provide assistance with investigations. This includes (but is not limited to) detectives with open cases, investigative units such as the Narcotics/Vice Division, and other outside agencies (i.e., Department of the Medical Examiner).

II. GUIDELINES

A. The Crime Analysis Unit (CAU) acts as a support detail and provides assistance for an ongoing criminal investigation and other types of inquiries. The assigned detective and detail shall continue to be responsible for the case.

B. Requests for facial recognition program services shall be submitted, via channels, to the Criminal Investigation Division (CID) on the Crime Analysis Request, HPD-107B form, with photograph(s) or video(s) to be reviewed. Photograph(s) and video(s) shall be handled as specified in Policy 8.13, HANDLING OF EVIDENCE AND FOUND PROPERTY.

Requests for expedited processing shall be indicated on the HPD-107B form in the OTHER/COMMENTS section.

C. The facial recognition program can examine various electronic media types for photographs and videos. Electronic media, including (but not limited to) thumb drives, compact discs, external hard drives, and hard copies, may be submitted with the request.

D. If the facial recognition system detects a viable candidate, the CAU shall complete a follow-up report for the assigned detective. The CAU analyst's follow-up report shall contain the steps taken to compare the known and unknown photographs and how the CAU analyst came to his or her conclusion(s).

E. In the event that a viable candidate cannot be located from the facial recognition system, the assigned detective will be notified that no candidate was identified.

F. If the CAU cannot discern a viable candidate, the photograph of the suspect will be considered unknown and remain in the facial recognition database system until:

1. A viable candidate is found;

2. The assigned detective notifies the CAU that the case has been completed, a viable candidate is no longer necessary, or the suspect has been found through other means; or

3. The statute of limitations has expired for the specific case.

III. FEDERAL BUREAU OF INVESTIGATION (FBI) DATABASE

If there is no match in the HPD's facial recognition program, the image may be sent to the FBI to search their Next Generation Identification (NGI) database. To request a search of the FBI's NGI database, the assigned detective shall submit a completed Crime Analysis Request, HPD-107B form, via channels, to the CID commander or designee.

IV. CAVEAT

Any results from the facial recognition system shall be used only as a guide for the investigation. The information provided does not constitute probable cause for an arrest. The results are only possible name(s) for the photograph(s) and video(s) that were submitted with the request. It shall be the responsibility of the assigned detective to verify the identity of all suspects.

V. AUTHORIZED USERS

Only departmental personnel who have been trained in the use of the facial recognition program shall access and use the system.

LOUIS M. KEALOHA
Chief of Police

Post on bulletin
board for one week

ACLU Hawai'i

Memorandum

Date: October 16, 2019
To: HCR225 Twenty-first Century Digital Privacy Law Task Force
From: George Cordero, American Civil Liberties Union of Hawai'i
Re: American Civil Liberties Union of Hawai'i Recommendations to HCR225 Twenty-first Century Digital Privacy Law Task Force

---

The American Civil Liberties Union of Hawai'i (ACLU of Hawai'i) is a private, non-profit, non-partisan organization with the mission to uphold and defend the civil rights and liberties in the federal and Hawai'i State Constitution. Privacy is one of the fundamental rights that the ACLU works to ensure the government does not violate. Technological innovation has far outpaced privacy protections that governments and corporations now have the capability to track our digital footprints in ways that were only once possible in sci-fi films. This memorandum will discuss the ACLU of Hawaii's concerns regarding the privacy implications of government use of face recognition technology (FRT) and will call on the HCR225 Twenty-first Century Digital Privacy Law Task Force (Task Force) to introduce proactive legislative provisions for a statewide ban. With the increasing number of cities and states enacting legislation to ensure constitutional protections from FRT, this memorandum explains several reasons the Task Force should adopt the prohibition safeguarding Hawai'i from dangerous, invasive, and biased systems that threaten civil rights and guarantee the legislature's constitutional obligation to uphold the right to privacy.

1. **Fourth amendment rights and first amendment-protected rights are at stake.**

FRT has a direct impact on people's Fourth Amendment rights and First Amendment-protected activities. The City and County of Honolulu recently approved increased surveillance in its tourist district and is working towards establishing more surveillance in its public parks. This surveillance footage could be used to build databases without people's knowledge and consent—increasing the potential for abuse. Even if people are not suspected of a crime, meeting certain physical attributes that society considers "threatening" (like engaging in political protest in public spaces) is sufficient enough to garner the attention of law enforcement. Hawaii's own history during World War II is a stark reminder that data gathered based on people's race, ethnicity, religious beliefs,

and political leanings, often lead to misuse, injustice, and the deterioration of civil rights and civil liberties protections.[1]

FRT enables the collection of not only biometric data, but also whereabouts, associations, and even facial expressions. Absent of notice and consent, the act of being in public allows for the unsolicited collection of photographs along with all their activities in social media.[2] The powerful and automated nature of FRT incentivizes the needless expansion of surveillance in communities. People should not have to be wary of having their movements and private lives recorded while in a public space. FRT can have a real chilling effect on people's willingness to engage in civic duties and exercise democratic values. In 2013, a study revealed that excessive policing and surveillance in Muslim communities in New York and New Jersey had a chilling effect on speech and association.[3] People actively decided to not visit mosques and limited their speech on social media. Excessive government surveillance through FRT disproportionally impact religious and political minority communities.

2. FRT threatens the civil rights of communities of color and women.

A recent test by the ACLU of Northern California reveals that FRT marketed to law enforcement mistakenly matched the faces of one out of five lawmakers with images from an arrest photo database. More than half of the falsely identified are lawmakers of color, which illustrates the most dangerous risk of FRT. A similar ACLU test conducted last year also misidentified 28 sitting members of Congress. There are also multiple studies that reveal the inaccuracies when used on women and people of color. An identification—whether accurate or not—could cost people their freedom or even their lives. People of color are already disproportionately harmed by police practices, and it's easy to see how FRT can exacerbate that.

3. The science behind FRT is far from perfect.

FRT is used to verify the identity of a person using facial characteristics. Algorithms determine distinctive details of each face—for example, the distance between the eyes or shape of the chin. This information is converted into a mathematical representation, given a template, and stored in a database.[4] Photos collected of an individual via social media,

---

[1]Cohen, A. (2011, May 5) Treatment of Japanese-Americans in WWII Hawaii Revealed in
[2]Donohue, L. (2012) Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age. Georgetown Law Faculty Publications and Other Works. Retrieved from https://scholarship.law.georgetown.edu/facpub/1036/
[3]Wasserman, M. (2015, November) First Amendment Limitations on Police Surveillance. Volume 90, Number 5. Retrieved from https://www.nyulawreview.org/issues/volume-90-number-5/first-amendment-limitations-on-police-surveillance/
[4]Lynch, J. (2018, February 12). Face Off: Law Enforcement Use of Face Recognition-Technology. Retrieved from https://www.eff.org/wp/law-enforcement-use-face-recognition.

police body cameras, surveillance cameras, traffic cameras, or in the field, are run against face templates in the database using algorithms that rely on facial markers to find the closest match. However, instead of yielding a single matching result, the system offers up several potential matches ranked in the order of likelihood of closest identification, which is extremely problematic.

Although databases used for the searches consists of mug shots, data sharing between government agencies are common, which also means access to non-criminal databases such as the DMV or the State Department.[5] Historically, these databases were primarily and exclusively comprised of photos of those who were previously involved in the criminal justice system. Using FRT against DMV databases can mean that biometric networks are being built using the photos the state's residents.

FRT is also heavily reliant on "perfect" conditions and produce negative results in poor lighting conditions, low resolutions, faulty angles, and etc. FRT's optimal performance relies on mug shot quality photographs with good lighting and from a frontal perspective.[6] When photographs are compared to those that have different lighting, shadows, backgrounds, poses, or expressions, the misidentification rate increases.[7] Identifying someone under low resolution or a in a video footage also poses the same issues. Misidentifications cause unnecessary interactions between law enforcement and innocent people often resulting to eroded trust, trauma, and serious harms.

4. Recommendation and Conclusion

It is our understanding that the Honolulu Police Department requires law enforcement officers to have reasonable suspicion to run a FRT search, with the exception for "requests that come directly from the Chief."[8] Right now, it is unclear whether searches can be run on witnesses or bystanders. Only FRT software certified staff are granted access to the system, and a Crime Analysis Unit staffer manually reviews potential matches.[9]

---

[5]McKinney, I. Biometrics: Facial Recognition. Retrieved from https://www.eff.org/document/biometrics-facial-recognition

[6]Lynch, J. (2018, February 12). Face Off: Law Enforcement Use of Face Recognition Technology. Retrieved from https://www.eff.org/wp/law-enforcement-use-face-recognition.

[7]Phillips, J., Beveridge, R., Draper, B., et al. An Introduction to the Good, the Bad, & the Ugly Face Recognition Challenge Problem. Retrieved from https://www.nist.gov/itl/iad/ig/upload/05771424.pdf

[8]Garvie, C., Bedoya, A., Frankle, J. (2016, October 8). The Perpetual Line-Up: Unregulated Police Face Recognition in America. Georgetown Law Center on Privacy and Technology. Retrieved from https://www.perpetuallineup.org/jurisdiction/hawaii

[9]Honolulu Police Department Policy Auxiliary and Technical Services, Policy Number 8.21, September 14, 2015 Retrieved from https://www.honolulupd.org/information/pdfs/FacialRecognitionProgram-02-04-2016-12-19-14.pdf

Hawai‘i is among the states that have determined that current statutes, rules, and regulations prohibit driver's license and ID card photos from being included in the FRT.[10]

Although Hawaii's current practice does not allow for the use of FRT for drivers licenses, it does not guarantee future protections. Regardless of how Hawai‘i agencies are *currently* using this technology, it is imperative that we safeguard our liberties in anticipation of future technological advancement or successive state administrations' or courts' interpretation of the law. **Due to the grave risks that FRT poses to our privacy, the ACLU of Hawai‘i strongly recommends a full ban on government use of this technology or use of information obtained through this technology.** This position is consistent with Hawai‘i law and stated policy. Hawai‘i is among the handful of states with explicit protections to the right to privacy incorporated within the State Constitution. Article I Sections 6 and 7 address the importance of the right to privacy and what constitutes as an invasion of privacy and also requires the Legislature to take affirmative steps to implement this right.[11]

While this technology may yield benefits for law enforcement through efficient collection of data and productive investigations, the costs of this technology to both civil rights and civil liberties substantially and categorically outweigh the benefits. The automatic and invasive tracking of our private lives through FRT poses a threat to our constitutional rights and will continue to be unchecked without legislation.

In May, the city of San Francisco became the first city to prohibit government acquisition and use of FRT. Since then, the cities of: Oakland, Berkley, Somerville, Cambridge have introduced and adopted similar legislation. More cities are beginning to understand the dangers and concerns of FRT and more will soon follow. Recently, the State of California successfully enacted a landmark law that blocks law enforcement from using FRT on body cameras. The ACLU of Hawai‘i recommends that the Legislature introduce similar legislation, codifying the permanent ban of the use of FRT or any information obtained from FRT not just in police body cameras but by any government agency or contractor statewide. It is integral that privacy protections keep up with technological advancements to ensure that the government continues to uphold our right to privacy. We must reclaim control of our information; for when privacy is at stake, free speech, security, and equality will soon follow.

---

[10]Garvie, C., Bedoya, A., Frankle, J. (2016, October 8). The Perpetual Line-Up: Unregulated Police Face Recognition in America. Georgetown Law Center on Privacy and Technology. Retrieved from https://www.perpetuallineup.org/jurisdiction/hawaii. See: attachment 016846, statement by Hawai‘i Criminal Justice Data Center Representative via email correspondence with Clare Garvie regarding the Driver's Privacy Protection Act and Real ID Act protections against FRT

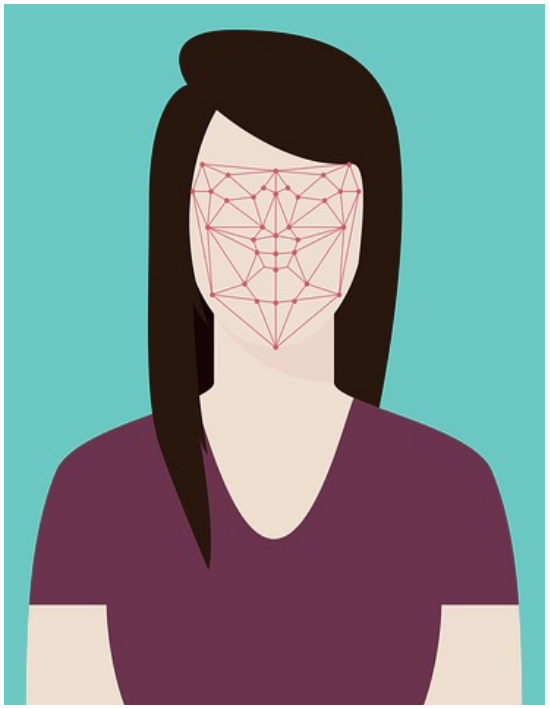
[11]See: The Constitution of the State of Hawai‘i. Article I. Section 6 and Section 7.

HCR225 Twenty-first Century Digital Privacy Law Task Force: Facial Recognition Technology (FRT) Presentation

ACLU Hawai'i

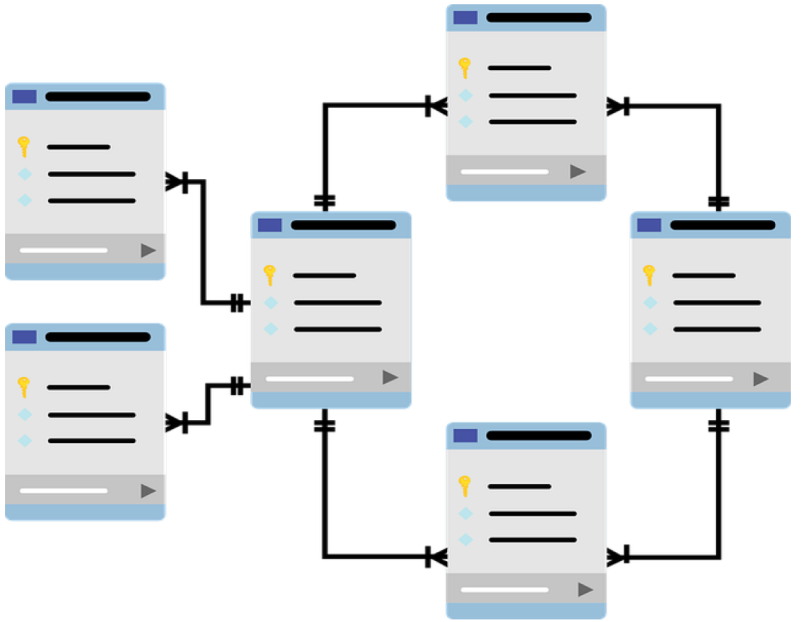
What is FRT and how does it work?

- Quick overview of concerns
- Biometric computer program
  - Analyzes images of human faces for purposes of identifying them
- Face template
  - Analyzes distance between eyes or shape of chin (face markers), compared with other templates



How is FRT used in Hawai‘i?

- HPD and FRT
  - Established in 2014 with Hawai‘i Criminal Justice Data Center, expanded to all counties in 2015 and access to database
  - Driver’s license photos are NOT included
- Reasonable Suspicion and Exception
  - FRT trained staff only
  - Results reviewed by Crime Analysis Unit
  - Unless request from directly from Chief
  - Requestor sends to FBI if no results
  - Run in FBI database



ACLU Concerns

- **Constitutional Rights Violations**
  - Threatens constitutional privacy rights and the 1st,4th, and 14th Amendments
- **Disproportionate Impacts**
  - Communities of color
  - Gender classifications
  - ACLU Study results
- **Accuracy Challenges**
  - Relies on “perfect” conditions
  - False positives and bias datasets

Constitutional Rights Violations

- Hawai‘i Constitution:
  - Explicit right to privacy
- Fourth Amendment
  - “Protects people, not places”
  - We do ”not surrender all 4th Amendment protection by venturing into the public…”
- First and Fourteenth Amendments
  - “Anonymity is a shield from the tyranny of the majority.”
  - “Awareness that government may be watching chills associational and expressive freedoms.”

Disproportionate Impacts

- Threatens communities of color
  - Misidentified ethnic minorities at higher rates
- Gender classification
  - 8.1% - 20.6% difference in male to female error rates
- ACLU Studies
  - ACLU NorCal Study on Legislative Members
  - ACLU National Study on Congressional members

Accuracy Challenges

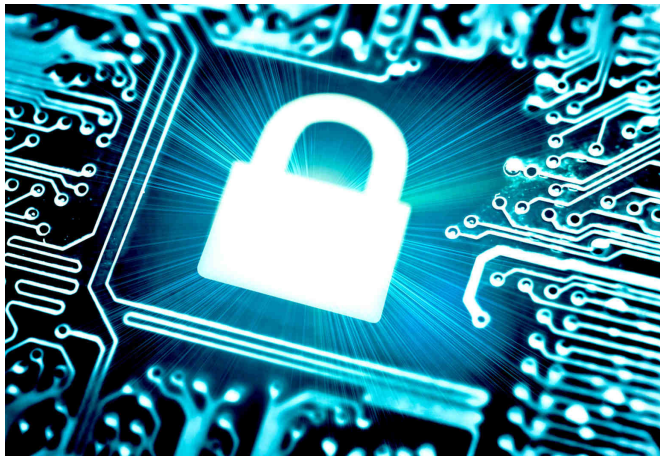
- Reliance on “perfect” conditions
  - Negative results in poor lighting, low resolutions, different angle, shadows, backgrounds, poses, facial expressions
- Biased Datasets
  - Not all benchmarks are created equal
- False positives
  - Offering several results instead of one rendering innocent suspects of a crime

FRT Laws

- No current Federal rules governing FRT
- California ban
  - Landmark law banning FRT use in police body cameras
- Cities and states everywhere
  - City Hall: San Francisco, Oakland, Berkeley, Somerville, Cambridge, Detroit, New York City
  - State Legislature: Massachusetts, Washington, New York, Michigan

Recommendations

- Follow the lead of of California and multiple cities and ban law enforcement use of facial recognition technology.
- Prohibit state and local government from sharing FRT data (including currently existing databases) with ICE or any other federal government agencies.
- Reaffirm that government use of FRT is incompatible with the Hawai‘i Constitution’s right to privacy.




ACLU
WE THE PEOPLE

LEGISLATIVE BRIEFING KIT

Depiction of individuals performing using digital or electronic technology: sexually explicit material: cause of action

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.

The Problem of Last-Minute Nudity Riders

This legislation establishes a clear framework for obtaining meaningful consent for such digitally produced sexually explicit material. It is a basic expectation that an individual sign a duly considered, negotiated nudity rider before being depicted in this way in any motion picture. It is a serious decision for any performer to do a nude scene, as it will forever affect their home life, career, public perception, fan base, or may affect their mental health. Any sexually explicit material should be carefully scripted and agreed-upon in advance. It is inappropriate to ambush a performer with a nudity rider on-set, away from an authorized personal representative or their labor union. These last-minute riders are a problem in the entertainment industry and any applicable law should legally prohibit them unless certain safeguards are satisfied.

Nudity Rider Requirements

Consent must be freely and knowingly given. The agreement must be written in plain language and provide a description of the planned sexually explicit material. In addition, one of the following must be satisfied:

- The nudity rider must be provided to the individual seventy-two hours in advance of signing; or
- The filmmaker must obtain written approval from the individual's attorney, talent agent, or manager, or if the individual does not have a personal representative, the approval of the labor union SAG-AFTRA; or
- If neither of these two requirements are satisfied, then the individual will have three days to submit written revocation of their consent.

Failure to obtain meaningful consent for these kinds of sexual depictions is a human rights violation. It does not matter if the film in question is shown on a porn website or is met with critical acclaim in the box office. The law should not provide filmmakers a creative license to harass, exploit, disparage, or demean.

Public Figures Provided Equal Protection

Sexually explicit material is not exempt from liability solely because the individual depicted is a public figure. Most of the videos produced are of public figures. Aspects of a person's life story may unfortunately make such material newsworthy; however, the sole fact that the individual is famous should explicitly not. Otherwise, this exemption would swallow the rule for the countless victims who work in the limelight.

Furthermore, this legislation provides plaintiffs the option of filing as a John Doe, Jane Doe, or Doe to maintain a certain level of confidentiality, if they so choose. An option that will be of particular importance to well-known victims who may wish to avoid the press coverage or inviting more people to view the offending content. A plaintiff may choose to be public about their lawsuit, particularly if they wish to let the public know the nude depiction was not real or that the bad actor producer created the content without consent.

A Disclaimer is Not a Defense

A filmmaker cannot simply provide a disclaimer or body double credit to avoid liability. Deepfakes porn, for example, is labeled fake, and a disclaimer would only serve to mitigate any claimed reputational harm damages.

Comprehensive Damages

The prevailing plaintiff will have access to economic and noneconomic damages and remedies:

- Lost wages.
- Reputational harm, including financial impact on performer's career. A performer who acts in kid's movies, for example, may have difficulty procuring new employment if they are associated with a sex scene.

- Emotional distress.
- The profits gained by the producer for producing the content OR statutory damages. In lieu of proving the profits gained by the producer, which is often speculative, the plaintiff can elect statutory damages instead. The judge has the discretion of awarding anywhere between $5,000 and $500,000. Statutory damages are in addition to any other economic or noneconomic damages available under this legislation.
- Punitive damages.
- Reasonable attorney's fees and costs.
- Any other available relief, including injunctive relief. It is critical victims of this content have a legal path to stop the content from being widely distributed. Once unlawful material of this kind enters mainstream distribution, the harm to the victim may be irreversible.

Statute of Limitations

A plaintiff has five years from the date they discover, or should have discovered, the sexually explicit material to bring a claim. Plaintiffs need time to know their rights, find an attorney, or be financially prepared to bring a lawsuit. Furthermore, any claim of a sexual nature will require more time as there are legitimate psychological and reputational factors to consider.

Press

Drew Harwell, "Fake-porn videos are being weaponized to harass and humiliate women: 'Everybody is a potential target,'" WASHINGTON POST December 30, 2018.

'[One victim of Deepfakes] felt nauseated and mortified: What if her co-workers saw it? Her family, her friends? Would it change how they thought of her? Would they believe it was a fake? 'I feel violated – this icky kind of violation,' said the woman, who is in her 40s and spoke on the condition of anonymity because she worried that the video could hurt her marriage or career. 'It's this weird feeling, like you want to tear everything off the Internet. But you know you can't.' Airbrushing and Photoshop long ago opened photos to easy manipulation. Now, videos are becoming just as vulnerable to fakes that look deceptively real. Supercharged by powerful and widely available artificial-intelligence software developed by Google, these like life "deepfake" videos have quickly multiplied across the internet, blurring the line between truth and lie. But the videos have also been weaponized disproportionately against women, representing a new and degrading means of humiliation, harassment and abuse."

Melanie Ehrenkranz, "The Screen Actors Guild Wants to Protect Its Members From Deepfakes," GIZMODO April 20, 2019.

"SAG-AFTRA's legal efforts would help ensure that its members, which include over 150,000 media workers, wouldn't have to worry about their images being exploited in death. And for the living, the union also said that it wants to 'support new judicial theories to extend protections to individuals and their heirs who are victimized in fake porn videos.' It's heartening to see a powerful organization fighting back against a gross form of both harassment and commercial

exploitation. As the tools to manipulate someone's image without their consent become cheaper and easier to use, it's hard to imagine why all states wouldn't want to adopt stronger protections for someone's likeness."

Samantha Cole, "Fake Porn Makers Are Worried About Accidentally Making Child Porn," MOTHERBOARD February 27, 2018

"If someone uses the faceset [collection of images of a person] that contains images of [Emma] Watson as a child to make a Deepfake, that means that a face of a minor was in part used to create a nonconsensual porn video. The people making Deepfakes and trading these facesets are worried about this. They write disclaimers that younger celebrities' facesets might contain photos of them as a minor. Some are deleting whole sets, such as one of Elle Fanning, until they can be sure it doesn't contain images of her as a minor. "I deleted all posts with Elle Fanning because it's impossible to prove that she was 18 years old in the old faceset," user Anton wrote on one Deepfakes forum. "It's better to be safe than sorry."

Joy Press, "Does Peak TV Have a Sex-Scene Problem?" VANITY FAIR December 21, 2018

"Many show-runners get little official training or guidelines before they step on set, and in an environment of tight budgets and increasing time pressure, decision-making can get messy. It can also lead shows to cut corners on rules – bullying actors into doing a sex scene or showing more flesh than they had contractually agreed to, for instance. According to David White, the executive director of actors' union SAG-AFTRA, "Our rules are clear, and there are decision-makers who, with an increasing regularity, are attempting to push those rules in order to achieve some creative or financial objective for their shows."

Question and Answer:

Don't filmmakers have First Amendment rights to create sexually explicit material of this kind without permission, no matter how vile or harmful?

They might, to a degree. The First Amendment is not absolute and Hawaii has a compelling interest to protect its residents from this form of image-based sexual abuse. Judges will likely be more sympathetic to individuals' need to protect their human dignity than they will be to a bad actor claiming creative expression. Unlike pornography of synthetic adults or children, which the U.S. Supreme Court has labeled protected speech, these videos depict a real human being's face. Thereby creating a real victim with real harms.

More so, this proposed legislation lays out explicit exemptions to liability, including disclosing material for a matter of legitimate public concern, for purposes of commentary or criticism, or inside of a work of political or newsworthy value.

Don't individuals have other laws and rights to protect themselves from these videos?

Maybe. It is uncertain, which is not good enough. Individuals need an explicit law with special rules around consent and remedies to target and discourage these videos. Individuals may be able to sue under other causes of action, if applicable. For example, defamation, false light, right of

publicity, or revenge porn laws are all patchwork state rights that serve independent, critical purposes of addressing image misuse.

- If a video is presented as real and there is actual reputational harm, the individual may be able to sue under defamation or false light. However, "Deepfake" porn videos labeled as such are inherently presented as false. Furthermore, defamation and false light disadvantage public figures.
- The individual may be able to sue under Hawaii's right of publicity law.
- In the United States, criminal revenge porn laws do not include protections for digitally created nudity. Furthermore, the *mens rea* required of these laws is often narrowed to personal relationships where the image was meant to be private and defendant knows the distribution will cause emotional harm. Most of these videos are created for sexual gratification or to make a profit.
- Since it is not the actual person's body parts, creating this content is likely not a privacy violation of any kind.
- If a film producer used this technology to depict an actor as naked without their consent in a movie, they may be able to sue the company under sexual harassment laws for creating a hostile work environment, as there was an employer-employee relationship present.
- If the unauthorized digital doubling occurs on a project covered by the SAG-AFTRA TV/TH Codified Basic Agreement, a performer hired by the company may utilize the CBA grievance arbitration process. However, the performer should speak to their legal representative and union SAG-AFTRA to determine if arbitration or litigation is the way to achieve their desired outcomes.

Legislation

LEGISLATIVE COUNSEL'S DIGEST

General Subject: Depiction of individuals performing using digital or electronic technology: sexually explicit material: cause of action.

Existing law creates a private right of action against a person who intentionally distributes a photograph or recorded image of another that exposes the intimate body parts of that person or of a person engaged in a sexual act without the person's consent if specified conditions are met.

This bill would also prohibit a person from intentionally disclosing sexually explicit material involving an individual depicted as performing. Depicted individual is defined as an identifiable, realistic replica of a human being that is created using digital or electronic technology, unless the depicted individual consented to the creation, development, and disclosure of that material. The bill would create a cause of action for an individual who suffers harm from the intentional disclosure of the sexually explicit material without the individual's knowingly and voluntarily obtained consent against a person who creates, develops, or discloses the sexually explicit material. The bill establishes special revocation rules around the timing of consent to discourage last minute nudity riders, including on a production set. Such last minute riders deny performers a meaningful opportunity to consider or review an agreement with their authorized personal representative or labor union. The bill would exclude from liability the disclosure of sexually explicit material under specified circumstances, including if the person disclosed the sexually explicit material in relation to a matter of legitimate public concern. The bill would establish procedures and requirements for bringing a cause of action under these provisions, including provisions on damages, the use of a pseudonym in pleadings, and requiring an action to be brought within a specified time.

Vote: majority. Appropriation: no. Fiscal committee: no.

PROPOSED:

(1) "Authorized Representative" means an attorney, talent agent, or personal manager authorized to present an individual or, if the individual does not have an attorney, talent agent, or personal manager, a labor union representing performers in audiovisual works.

(2) "Consent" or "consented" means a written agreement, written in plain language, signed knowingly and voluntarily by the individual that includes a description of the sexually explicit material and the audiovisual work in which it will be incorporated, and that complies with one or more of the following:

(A) The individual is given at least 72 hours to review the terms of the agreement before signing it; or

(B) The individual's authorized representative, if the depicted individual has one, provides written approval of the signed agreement; or

(C) The individual has three days after signing the agreement to rescind the consent by providing written notice.

(3) “Depicted individual” means an identifiable, realistic replica of a human being that is created using digital or electronic technology, including, but not limited to, depicting the body parts of another human being as being those of the individual.

(4) “Disclose” means to transfer, publish, make available, or distribute.

(5) “Harm” includes, but is not limited to, economic harm or emotional distress.

(6) “Individual” means a natural person.

(7) “Nude” means visible genitals, pubic area, anus, or a female’s post-pubescent nipple of areola.

(8) “Person” means a human being or legal entity.

(9) “Sexual conduct” means any of the following:

(A) Masturbation.

(B) Sexual intercourse, including genital, oral, or anal, whether between persons regardless of sex or gender or between humans and animals.

(C) Sexual penetration of the mouth, vagina, or rectum by, or with, an object.

(D) The transfer of semen onto the depicted individual.

(E) Sadomasochistic abuse involving the depicted individual.

(10) “Sexually explicit material” means any portion of an audiovisual work that shows the depicted individual performing in the nude or appearing to engage in, or being subjected to, sexual conduct.

(b)

(1) A person shall not intentionally disclose sexually explicit material involving a depicted individual unless the individual consented to the creation, development, or disclosure of the sexually explicit material.

(2) An individual who has suffered harm resulting from the intentional disclosure of sexually explicit material involving a depicted individual without the individual’s consent has a cause of action against a person who creates, develops, or discloses the sexually explicit material, or any audiovisual works in which the sexually explicit material is incorporated, if the person knew or reasonably should have known the individual did not consent to the creation, development, and disclosure of the sexually explicit material.

(c)

(1) A person is not liable under this section if the person proves any of the following:

(A) The person disclosed the sexually explicit material in the course of reporting unlawful activity, in the course of a legal proceeding, or the person is a member of law

enforcement and disclosed the sexually explicit material in the course of exercising the person's law enforcement duties.

(B) The person disclosed the sexually explicit material in relation to a matter of legitimate public concern.

(C) The person disclosed the sexually explicit material in a work of political or newsworthy value, or similar work.

(D) The person disclosed the sexually explicit material for the purposes of commentary or criticism or the disclosure is otherwise protected by the Hawaii Constitution or the United States Constitution.

(2) For purposes of this subdivision, sexually explicit material is not of newsworthy value solely because the individual is a public figure.

(d) It shall not be a defense to an action under this section that there is a disclaimer included in the sexually explicit material that communicates that the inclusion of the depicted person in the sexually explicit material was unauthorized or that the individual did not participate in the creation or development of the material.

(e)

(1) A prevailing plaintiff may recover any of the following:

(A) Economic or noneconomic damages proximately caused by the disclosure of the sexually explicit material, including damages for emotional distress.

(B) An amount equal to the monetary gain made by the defendant from the creation, development, or disclosure of the sexually explicit material, or the plaintiff may, at any time before the final judgment is rendered, recover instead an award of statutory damages for all unauthorized acts involved in the action, with respect to any of one work, in a sum not less than five thousand dollars ($5,000) or more than five hundred thousand dollars ($500,000).

(C) Punitive damages.

(D) Reasonable attorney's fees and costs.

(E) Any other available relief, including injunctive relief.

(2) This act does not affect any right or remedy available under any other law.

(f) An action under this section shall be brought no later than five years from the date the unauthorized creation, development, or disclosure was discovered or should have been discovered with the exercise of reasonable diligence.

(g)

(1) A plaintiff may proceed using a pseudonym, either John Doe, Jane Doe, or Doe, for the true name of the plaintiff and may exclude or redact from all pleadings and documents filed in the

action other identifying characteristics of the plaintiff. A plaintiff who proceeds using a pseudonym and excluding or redacting identifying characteristics as provided in this section shall file with the court and serve upon the defendant a confidential information form for this purpose that includes the plaintiff's name and other identifying characteristics excluded or redacted. The court shall keep the plaintiff's name and excluded or redacted characteristics confidential.

(2) In cases where a plaintiff proceeds using a pseudonym under this section, the following provisions shall apply:

(A) All other parties and their agents and attorneys shall use this pseudonym in all pleadings, discovery documents, and other documents filed or served in the action, and at hearings, trial, and other court proceedings that are open to the public.

(B)

(i) Any party filing a pleading, discovery document, or other document in the action shall exclude or redact a pleading, discovery document, or other document, except for a confidential information form filed pursuant to this subdivision.

(ii) A party excluding or redacting identifying characteristics as provided in this section shall file with the court and serve upon all other parties a confidential information form that includes the plaintiff's name and other identifying characteristics excluded or redacted. The court shall keep the plaintiff's name and excluded or redacted characteristics confidential.

(C) All court decisions, orders, petitions, discovery documents, and other documents shall be worded so as to protect the name or other identifying characteristics of the plaintiff from public revelation.

(3) The following definitions apply to this subdivision:

(A) "Identifying characteristics" means name or any part thereof, address or any part thereof, city or unincorporated area of residence, age, marital status, relationship to defendant, and race or ethnic background, telephone number, email address, social media profiles, online identifiers, contact information, or any other information, including images of the plaintiff, from which the plaintiff's identity can be discerned.

(B) "Online identifiers" means any personally identifying information or signifiers that would tie an individual to a particular electronic service, device, or Internet application, website, or platform account, including, but not limited to, access names, access codes, account names, aliases, avatars, credentials, gamer tags, display names, handles, login names, member names, online identities, pseudonyms, screen names, user accounts, user identifications, usernames, Uniform Resource Locators (URLs), domain names, Internet Protocol (IP) addresses, and media access control (MAC) addresses.

(4) The responsibility for excluding or redacting the name or identifying characteristics of the plaintiff from all documents filed with the court rests solely with the parties and their attorneys.

Nothing in this section requires the court to review pleadings or other papers for compliance with this provision.

(5) Upon request of the plaintiff, the clerk shall allow access to the court file in an action filed under this section only as follows:

(A) To a party to the action, including a party's attorney.

(B) To a person by order of the court on a showing of good cause for access.

(h) The provisions of this section are severable. If any provision of this section or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.

October 18, 2019

The Honorable Michelle N. Kidani
The Honorable Chris Lee
Hawaii State Capitol
415 South Beretania St
Honolulu, HI 96813

Dear Co-Chairs Kidani and Lee:

Internet Association appreciates the opportunity to provide the "21st Century Privacy Law Task Force" some initial comments regarding your consideration of several discrete topics related to consumer data privacy.

Internet Association (IA) represents more than 40 of the world's leading internet companies and advances public policy solutions that foster innovation, promote economic growth, and empower people through the free and open internet.

IA companies believe trust is fundamental to their relationship with individuals. Our member companies know to be successful they must meet individuals' reasonable expectations with respect to how the personal information they provide to companies will be collected, used, and shared. That is why our member companies are committed to transparent data practices, and to continually refining their consumer-facing policies so that they are clear, accurate, and easily understood by ordinary individuals. Additionally, our member companies have developed numerous tools and features to make it easy for individuals to manage the personal information they share, as well as their online experiences.

As your Task Force begins examining several privacy-related topics, IA recommends focusing your efforts on issues where a current, tangible privacy harm can be identified, where meaningful privacy gains can be provided to consumers in response, and where any new obligations on businesses are clear and workable.

Additionally, IA cautions against rushing to legislate without a thorough and thoughtful process. As has been seen in California, a rush to legislate in 2018 has led to yet another privacy initiative that will appear on the 2020 ballot, leaving consumers and businesses in a complete state of uncertainty. In contrast, the Oregon Attorney General has formed a Consumer Privacy Task Force, made up of a variety of stakeholders, with the intent of developing legislation to be introduced in the 2021 legislative session. IA suggests ensuring your process similarly allows for meaningful discussion and understanding before you move forward with any legislation.

IA appreciates the opportunity to provide comments to the 21st Century Task Force and welcome an opportunity to work with you to develop meaningful consumer data privacy legislation. If you have any questions please reach out to me at rose@internetassociation.org or 206-326-0712.

Thank you for your consideration.

Sincerely,

Rose Feliciano
Director, State Government Affairs Northwest Region

Additional Material
HCR225 Twenty-first Century Privacy Law Task Force
Monday, October 21, 2019

General:

INTERVIEW: Data-privacy compliance timeline is 'yesterday,' leading tech lawyer says. Reuters, October 10, 2019.

Data Breaches:

Probe finds no unauthorized access to Hawaii public school student data. Star Advertiser, September 6, 2019.

It's not just Equifax: Here's every major security breach and data hack so far. CNET, August 5, 2019.

Data Breaches Expose 4.1 Billion Records in First Six Months of 2019. Forbes, August 20, 2019.

Data Brokers:

The Data Brokers So Powerful Even Facebook Bought Their Data – But They Got Me Wildly Wrong. Forbes, April 5, 2018.

What Are 'Data Brokers,' and Why Are They Scooping Up Information About You? Vice, March 27, 2018.

A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes. United States Senate Office of Oversight and Investigations, Majority Staff, December 18, 2013.

Facial Recognition:

What happens when employers can read your facial expressions. New York Times, October 17, 2019.

Data regulator probes King's Cross facial recognition tech. BBC, August 15, 2019.

Facial recognition software mistook 1 in 5 California lawmakers for criminal says ACLU. Los Angeles Times, August 13, 2019.

Facial Recognition is Accurate, if You're a White Guy. New York Times, February 8, 2018.

Deepfakes:

What ‘deepfakes’ are and how they may be dangerous. CNBC, October 13, 2019.

This deepfake shows an impressionist taking on 20 celebrities, convincingly. CNET, October 10, 2019.