

OUR PEOPLE

Overview My Service My Library

HOWARD J. SYMONS

Partner

WASHINGTON, DC

Phone: 202 639-6078

hsymons@jenner.com

Download V-Card

PRACTICE GROUPS

Communications, Internet and Technology

EDUCATION

Harvard Law School, J.D., 1978

Yale University, B.A., 1975; *summa cum laude*

ADMISSIONS

District of Columbia

COURT ADMISSIONS

U.S. Supreme Court

U.S. Court of Appeals, Second Circuit

U.S. Court of Appeals, Fourth Circuit

U.S. Court of Appeals, Sixth Circuit

U.S. Court of Appeals, Ninth Circuit

U.S. Court of Appeals, Tenth Circuit

U.S. Court of Appeals, District of Columbia Circuit

U.S. District Court, District of Columbia

Howard J. Symons is a partner in the Communications, Internet & Technology Practice. He has nearly 40 years of experience in telecommunications law and policy, including senior positions in government and the private sector. Before joining the firm in 2017, he served in two high-profile roles at the Federal Communications Commission: as general counsel from 2016 to 2017 and as vice-chair of the FCC's Incentive Auction Task Force from 2014 to 2016. He was appointed to both posts by Chairman Tom Wheeler.

Highly regarded throughout the industry, Mr. Symons has represented companies in the cable, wireless and telecommunications industries as well as their trade associations before the FCC, Congress and State legislatures, and the courts. Mr. Symons advised these companies on a wide range of matters, including video, broadband and telephony.

As general counsel of the FCC, Mr. Symons oversaw more than 60 lawyers that provide legal support for the Commission's policy and rulemaking activities and recommend decisions in adjudicatory matters. He also served as one of Chairman Wheeler's four senior advisors. As vice chair of the Incentive Auction Task Force, he was one of the primary architects of the first incentive auction: a two-sided auction in which broadcasters bid to give up their spectrum and wireless providers bid to buy it.

From 1985 to 2014, Mr. Symons was a partner at another AmLaw 100 firm, chairing that firm's communications practice and serving as a member of the Policy (Executive) Committee. From 1981 to 1985, he served as senior counsel to the Subcommittee on Telecommunications in the US House of Representatives; in that role, he was responsible for developing legislation on matters ranging from domestic telephone policy to cable franchising and international telecommunications.


Mr. Symons also served as an adjunct professor at George Washington University's National Law Center, where he taught courses in telecommunications law and regulation for 10 years. He has authored several articles on the telecommunications policy process, testified before Congress and state legislatures, and spoken at numerous industry conferences and continuing legal education seminars on topics relating to regulatory trends, the FCC and more.





Charter has called for a strong, national framework to protect consumers' privacy online. Consumers need better tools to control how their information is collected and used regardless of what online services they use or where they are when they go online.

Consumers will be best protected by a national online privacy framework that empowers them to control the personal information that is collected about them online.


It should focus on five core principles:

- 

Parity: Consumers are best served by a uniform framework that is applied consistently across the entire Internet ecosystem. The same type of personal data should not be protected differently based on the business model of the entity collecting the data. Different policies that lead to inconsistent protections create confusion and erode consumers' confidence in their interactions online, threatening the continued growth of today's digital economy. Moreover, regulations that disfavor one technology or business model over another would deter market entry, thwart innovation and limit competition.
- 

Control: Consumers should have meaningful choice for use of their data through opt-in consent. No more pre-checked "boxes" or take-it-or-leave-it offers. The use of personal data should be reasonably limited to deliver the service the consumer engaged in.
- 

Transparency: Consumers should be given the information they need to make informed decisions. How companies collect, use and maintain consumers' data should be clear, concise, easy-to-understand and readily available.
- 

Uniformity: There should be a single national standard that protects consumers' online privacy regardless of where they live, work or travel. A patchwork of state laws would be confusing for consumers, difficult for businesses to implement, and hinder continued innovation on the internet—which is a borderless technology.
- 

Security: Privacy is security and security is privacy. Strong data security practices should include administrative, technical and physical safeguards to protect against unauthorized access to personal data, and ensure that these safeguards keep pace with technological development.

ISPs

List of current bills

CT SB 6	Failed	Requires Internet service providers to register and pay registration fees and require the Public Utilities Regulatory Authority to apply net neutrality principles to Internet service providers and enforce such principles with civil penalties and to prohibit certain telecommunications companies, certified telecommunications providers, certified competitive video service providers and Internet service providers from collecting personal information.
CT HB 6601	Failed	Concerns data privacy and minors, requires Internet social media platforms to remove content created by individuals under the age of eighteen at such individuals request, prohibits such platforms and Internet web sites that primarily engage minors from advertising products or services that are illegal for minors to purchase, and if such advertising is targeted toward a minor based on personal information collected regarding such minor.
HI HB 2296 (2018)	Failed	Prohibits internet service providers from using the personal information of customers for specific purposes without the prior written consent of customers.
LA HB 465	Failed	Creates the Internet and Social Media Data Privacy and Protection Act to protect consumer's private confidential information that is obtained by internet, broadband, and social media companies.
MA SB 1936	Pending	Promotes net neutrality and consumer protection. Provides customers with a mechanism to easily opt-out of third-party access to customer proprietary information for purposes other than the provision of broadband internet access service from which that customer proprietary information was derived.
MD HB 141	Failed	Specifies the circumstances under which a broadband internet access service provider may handle certain customer personal information, establishes a mechanism through which a broadband Internet access service provider may obtain customer consent to have certain personal information handled in a certain manner.
ME SB 275	Enacted Effective 7/1/2020	Prohibits a provider of broadband Internet access service from using, disclosing, selling, or permitting access to customer personal information unless the customer expressly consents to such, provides other exceptions under which a provider may use, disclose, sell, or permit access to customer personal information, prohibits a provider from refusing to serve a customer, charging a customer a penalty, or offering a customer a discount.

MN SB 1553	Pending	Relates to commerce, requires telecommunications service providers to comply with Internet privacy requirements, defines terms and modifying definitions, requires express approval of disclosure of personally identifiable information, increases civil liability threshold.
MT HB 457	Failed	Protects the privacy of internet access service customers, requires prior affirmative consent before an internet access service provider may use a customer's personal information, provides definitions and exceptions, provides for enforcement and penalties, and authorizes rulemaking.
NJ AB 1527 SB 2641	Pending	Requires internet service providers to keep confidential and prohibit any disclosure, sale, or unauthorized access to subscriber's personally identifiable information unless subscriber authorizes Internet service provider in writing to disclose information.
NJ AB 1927	Pending	Requires Internet service providers to keep confidential subscriber's personally identifiable information unless subscriber authorizes Internet service provider in writing or email to disclose information, prohibits subscriber penalty.
NJ AB 3711	Pending	Requires internet service providers to keep confidential subscriber's personally identifiable information unless subscriber authorizes Internet service provider in writing to disclose information.
NY AB 2420 SB 518	Pending	Prohibits the disclosure of personally identifiable information by an internet service provider without the express written approval of the consumer.
NY AB 3612	Pending	Requires internet service providers to provide customers with a copy of their privacy policy and to obtain written and explicit permission from a customer prior to sharing, using, selling or providing to a third party any sensitive information of such customer.
NY SB 5245	Pending	Relates to the sale of personal information by an internet service provider.
NY SB 1180	Pending	Prohibits internet service providers from disclosing personally identifiable information where a consumer requests that his or her information not be disseminated, defines terms, makes exceptions, and imposes a civil penalty.
SC HB 3339	Pending	Provides that a telecommunications or internet service provider that has entered into a franchise agreement, right of way agreement, or other contract with the state of South Carolina or one of its political subdivisions, or that uses facilities that are subject to those agreements, even if it is not a party to the agreement, may not collect personal information from a customer resulting from the customer's use of the telecommunications.

	FCC 2016 Privacy Order	CT SB 6	CT HB 6601	HI HB 2296 (2018)	LA HB 465	MA SB 1936	MD HB 141	ME SB 275	MN SB 1553	MT HB 457	NJ AB 1527	NJ AB 1927	NJ AB 3711	NY AB 2420	NY AB 3612	NY SB 5245	NY SB 1180	SC HB 3339
Status applies to		Failed	Failed		Failed	Pending	Failed	Enacted	Pending	Failed	Pending	Pending	Pending	Pending	Pending	Pending	Pending	Pending
Internet Service Providers	X	X		X	X	X	X	X	Enacted		X	X	X	X	X	X	X	X
telecom companies	X	X							X		X				X	X	X	X
social media registry			X		X													
net neutrality		X				grade, seal												
limitations on collection of PII		X																opt-in
limitations on sharing of PII	opt-in sensitive opt-out non-			opt-in	opt-in	opt-out	opt-out	opt-in	opt-in	opt-in	opt-in	opt-in	opt-in	opt-in	opt-in	opt-in	opt-in	opt-out
limitation on retention				reasonably necessary			reasonably											
restriction on targeted advertising			minors	opt-out			opt-out			opt-out								
right to deletion			minors															
consumer notice	X			X	X		X	X			X	X	X		X	X	X	
private right of action					X													
security program	X			X				X	X					X				
breach notification																		
data covered includes	any		any	any		any	any	any	expands		any	any	any		any	any		
geolocation	sensitive			X	X	X	X	X	X		X							
browsing history, app data	sensitive			X	X	X		X	X	X	X	X	X	X	X	X	X	X
finer or fees	X			X					increases	X				X	X	X	X	

The background features abstract, overlapping green geometric shapes in various shades, creating a modern and dynamic look. The shapes are primarily triangles and polygons, some with thin white outlines, set against a white background.

Summary Internet Service Provider (ISP) Privacy Law and Legislation

Kelly McCanlies, FIP, CIPP/US, CIPM, CIPT

Agenda

- ▶ Common Terms
- ▶ Laws
 - ▶ Federal
 - ▶ State
- ▶ Legislation
 - ▶ Federal
 - ▶ State

Common Terms

▶ Internet Service Provider (ISP)

An ISP is a company such as AT&T, Verizon, or Comcast, that provides Internet access to companies, families, and even mobile users. ISPs use fiber-optics, satellite, copper wire, and other forms to provide Internet access to its customers.

▶ Common Carrier

A **common carrier**, in telecommunications, is an entity that provides wired and wireless communication services to the general public for a fee. ... In the United States, the **common carrier** designation made by the Federal Communications Commission (FCC), under authorization of the **Communications Act of 1934**.

▶ Voice over Internet Protocol (VoIP)

Also called IP telephony, is a method and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.

A landline telephone is the traditional wired phone. ... VoIP on the other hand, uses an IP phone or a softphone to make calls over the Internet. A VoIP phone converts the sound of your voice into data packets and then sends them to the target destination.

Law - Federal

- ▶ **Communications Act of 1934**
- ▶ **1996 Telecommunications Act**
 - ▶ FCC - Regulates telecommunications companies as common carriers
 - ▶ Customer Proprietary Network Information (CPNI)
(e.g., phone numbers called; the frequency, duration, and timing of such calls; and any services purchased by the consumer)
 - ▶ Covers telephone calls
- ▶ **FCC's 2007 CPNI Order**
 - ▶ Opt-in to share CPNI with third-party marketing firms
 - ▶ Opt-out to share CPNI with affiliated communications firms
 - ▶ Extended CPNI to VOIP (Voice over IP) service

In 2015, the FCC reclassified broadband providers as telecommunication carrier

- ▶ **FCC's 2016 Privacy Order**
 - ▶ Extended CPNI regulations to broadband internet access services
 - ▶ On 4/3/2017 - repealed by US Congressional joint resolution

Law - Federal

- ▶ FTC (Federal Trade Commission Act of 1914)
 - ▶ FTC v. AT&T Mobility LLC
 - ▶ 2014 - enforcement action on throttling speed of unlimited data
 - ▶ 2015 - FCC reclassified mobile data service as a common carrier service
 - ▶ 2016 -AT&T appealed, saying it was exempt from FTC authority because of common carrier **status**. 9th Circuit Court of Appeals agreed
 - ▶ 2018 - 9th Circuit Court of Appeals - en banc reversal
 - Because common carrier designation is **activity** based, common carrier exemption is also activity based
 - ▶ March 2019 - FTC announces broadband privacy study - 7 companies
 - ▶ August 2019 - scope expanded to additional companies

Law - State

- ▶ Minnesota: [Chapter 325M. Internet Privacy](#) (2002)
 - ▶ Prohibits ISPs from sharing PII (physical or electronic address, browser history, contents of a customer's data storage device)
 - ▶ Allows disclosure with consent or for subpoena, court order, etc.
 - ▶ Requires ISPs to have reasonable security
 - ▶ Allows an individual to bring action with awards of \$500 or actual damage, does not allow class actions
- ▶ Nevada [NRS 205.498](#) (1999)
 - ▶ Applies to provider who charges for internet service or electronic mail address
 - ▶ Opt-in - Must keep confidential all information (other than email address), unless consent is given
 - ▶ Opt-out - Permits sharing of email address unless consent is withdrawn
 - ▶ Notice of write to limit sharing of email address
 - ▶ Misdemeanor and a fine of \$50 - \$500 per violation
- ▶ California: CCPA (2018)

Legislation - Federal

- ▶ S.3744 - Data Care Act of 2018 (Sen. Brian Schatz)
 - ▶ Defines key terms “individual identifying data” and “sensitive information”
 - ▶ Enforcement by the FTC
 - ▶ Duties of online service providers: “duties of care, loyalty, and confidentiality” to end users.
 - ▶ Duty of care: “reasonably secure individual identifying data from unauthorized access” and promptly inform them of any data breaches.
 - ▶ Duty of loyalty: a company could not use individual identifying data in a way that would
 - “benefit the online service provider to the detriment of an end user,”
 - “result in reasonably foreseeable and material physical or financial harm to an end user” or
 - “be unexpected and highly offensive to a reasonable end user.”
 - ▶ Duty of confidentiality: impose restrictions on the disclosure and sale of individual identifying information to third parties.
 - ▶ Includes non-profits and common carriers

Legislation - Federal

- ▶ Privacy Bill of Rights Act
 - ▶ Substantially similar to CCPA
- ▶ Do Not Track Act
 - ▶ Substantially similar to federal Do Not Call Act

Specific areas of risk identified by Task Force members or interested stakeholders:

- Expanding the HRS definition of personal information (section 487N-1)
 - Proposed draft language (Most recent version circulated 11/26)
- Regulation or registration of data brokers; opt-in to sale of information
 - Proposed draft language (First circulated 11/26)
- Sale of geolocation data
 - Proposed draft language (First circulated 11/26)
- Law enforcement's access to data by search warrant; Disclosure of court release of data to users
 - Proposed draft language (First circulated 9/26)
- Deep fakes
 - Proposed draft language by CCH Prosecutor's Office (First circulated 10/27)
 - Proposed draft language by SAG-AFTRA (First circulated 11/4)
- Facial recognition technology
- Internet Service Provider privacy
- Private right of action for privacy statute business violations
- Right to deletion

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

Created from examples from 11 state laws (below).

"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**. (See **notes from November 15 meeting**)
 - (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**. (See **notes from November 15 meeting**)
 - (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. (See **notes from November 15 meeting**)
-

Sept. meeting - Examples of Other State Laws

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.

Nov. 15 meeting – Answers to questions from October

Last 4 of SSN / TIN

- The first three digits are known as the "**Area Number**". Until June 25, 2011, this is generally the State or territory where your SSN was assigned. Thereafter, the number was randomly assigned.
- The second two numbers are known as the "**Group Number**". They really do not have any geographical or data significance.
- The third set of four numbers is simply the numerical sequence of digits 0001 to 9999 issued within each group.

People born in the United States since 1987 may have had their SSN applied for them by the hospital at birth. This policy varies by State.

Hawaii Area Numbers	Group Numbers	
575	01-99	1935 - 2004
576	01-99	1935 - 2004
750	01,03,05,07,09,10,12,14,16,18,20	2004 - 2011
751	01,03,05,07,09,10,12,14,16,18	2004 - 2011

<https://www.ssn-verify.com/lookup/hawaii>

From IRS.gov

“Examples of PII include, but are not limited to:

- a. Name, such as full name, maiden name, mother’s maiden name, alias, or name control (first 4 letters of last name).
- b. Address information, such as street address or email address.
- c. A unique set of numbers or characters assigned to a specific individual, such as:
 1. Telephone numbers, including mobile, business, and personal numbers.
 2. SSN, **including the last 4 digits**.
 3. Taxpayer identification number (TIN) that identifies an individual.”

From HHS.gov (HIPAA)

“a data set that contained ... the last four digits of a Social Security number, would not meet the requirement ... for de-identification.”

Digital Signature

Electronic signatures are a legal concept distinct from **digital signatures**, a cryptographic mechanism often used to implement electronic signatures. While an electronic signature can be as simple as a name entered in an electronic document, digital signatures are increasingly used in e-commerce and in regulatory filings to implement electronic signatures in a cryptographically protected way.

- Arizona: A private key that is unique to an individual and that is used to authenticate or sign an electronic record.
- North Carolina: Digital signatures.
- Alternative wording?

A digital signature **used to create an electronic signature** or private key that is unique to an individual and that is used to authenticate or sign an electronic record.

Or omit digital signature?

Data Brokers

Proposal

An act relating to data brokers and consumer protection

FINDINGS AND INTENT

(a) The General Assembly finds the following:

(1) Providing consumers with more information about data brokers, their data collection practices, and the data collected relating to the consumer.

(A) While many different types of businesses collect data about consumers, a “data broker” is in the business of aggregating and selling data about consumers with whom the business does not have a direct relationship.

(B) A data broker collects many hundreds or thousands of data points about consumers from multiple sources, including: Internet browsing history; online purchases; public records; location data; loyalty programs; and subscription information. The data broker then scrubs the data for accuracy; analyzes the data to assess content; and packages the data for sale to a third party.

(C) Data brokers provide information that is critical to services offered in the modern economy, including: targeted marketing and sales; credit reporting; background checks; government information; risk mitigation and fraud detection; people search; decisions by banks, insurers, or others whether to provide services; ancestry research; and voter targeting and strategy by political campaigns.

(D) While data brokers offer many benefits, there are also risks associated with the widespread aggregation and sale of data about consumers, including risks related to consumers’ ability to know and control information held and sold about them and risks arising from the unauthorized or harmful acquisition and use of consumer information.

(E) There are important differences between “data brokers” and businesses with whom consumers have a direct relationship.

(i) Consumers who have a direct relationship with traditional and e-commerce businesses may have some level of knowledge about and control over the collection of data by those businesses, including: the choice to use the business’s products or services; the ability to review and consider data collection policies; the ability to opt out of certain data collection practices; the ability to identify and contact customer representatives; the ability to pursue contractual remedies through litigation; and the knowledge necessary to complain to law enforcement.

(ii) By contrast, consumers may not be aware that data brokers exist, who the companies are, or what information they collect, and may not be aware of available recourse.

(F) To provide consumers with necessary information about data brokers, Hawaii should adopt a narrowly tailored definition of “data broker” and require data brokers to register annually with the Attorney General and provide information about their data collection activities, opt-out policies, purchaser credentialing practices, and security breaches.

(2) Ensuring that data brokers have adequate security standards.

(A) News headlines in the past several years demonstrate that large and sophisticated businesses, governments, and other public and private institutions are constantly subject to cyberattacks,

which have compromised sensitive personal information of literally billions of consumers worldwide.

(B) While neither government nor industry can prevent every security breach, the State of Hawaii has the authority and the duty to enact legislation to protect its consumers where possible.

(C) One approach to protecting consumer data has been to require government agencies and certain regulated businesses to adopt an “information security program” that has “appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records” and “to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm.” Federal Privacy Act; 5 U.S.C. § 552a.

(D) The requirement to adopt such an information security program currently applies to “financial institutions” subject to the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq; to persons who maintain or transmit health information regulated by the Health Insurance Portability and Accountability Act; and to various types of businesses under laws in at least 13 other states.

(E) Hawaii can better protect its consumers from data broker security breaches and related harm by requiring data brokers to adopt an information security program with appropriate administrative, technical, and physical safeguards to protect sensitive personal information.

(3) Prohibiting the acquisition of personal information through fraudulent means or with the intent to commit wrongful acts.

(A) One of the dangers of the broad availability of sensitive personal information is that it can be used with malicious intent to commit wrongful acts, such as stalking, harassment, fraud, discrimination, and identity theft.

(B) While various criminal and civil statutes prohibit these wrongful acts, there is currently no prohibition on acquiring data for the purpose of committing such acts.

(C) Hawaii should create new causes of action to prohibit the acquisition of personal information through fraudulent means, or for the purpose of committing a wrongful act, to enable authorities and consumers to take action.

(b) Intent.

(1) Providing consumers with more information about data brokers, their data collection practices, and the right to opt out. It is the intent of the General Assembly to provide state residents with access to more information about the data brokers that collect consumer data and their collection practices by:

(A) adopting a narrowly tailored definition of “data broker” that:

(i) includes only those businesses that aggregate and sell the personal information of consumers with whom they do not have a direct relationship; and

(ii) excludes businesses that collect information from their own customers, employees, users, or donors, including: banks and other financial institutions; utilities; insurers; retailers and grocers; restaurants and hospitality businesses; social media websites and mobile “apps”; search websites; and businesses that provide services for consumer-facing businesses and maintain a direct relationship with those consumers, such as website, “app,” and e-commerce platforms; and

(B) requiring a data broker to register annually with State of Hawaii's office of consumer protection and make certain disclosures in order to provide consumers, policy makers, and regulators with relevant information.

- (2) Ensuring that data brokers have adequate security standards. It is the intent of the General Assembly to protect against potential cyber threats by requiring data brokers to adopt an information security program with appropriate technical, physical, and administrative safeguards.
- (3) Prohibiting the acquisition of personal information with the intent to commit wrongful acts. It is the intent of the General Assembly to protect state residents from potential harm by creating new causes of action that prohibit the acquisition or use of personal information for the purpose of stalking, harassment, fraud, identity theft, or discrimination.
- (4) Recognizing that credit reporting agencies present special risks to consumers' financial well-being and that federal law provides for special access and rights for consumers to their personal information held by credit reporting agencies, it is the intent of the General Assembly to promote consumer awareness of these rights.

DEFINITIONS

- (1) "Personal information" means an Identifier in combination with one or more Specified Data Elements.
- (A) 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.
- (B) "Specified Data Element" means any of the following:
- (i) An individual's social security number, either in its entirety or the last four digits.
 - (ii) Driver's license number, federal or state identification card number, or passport number.
 - (iii) An individual's federal or State of Hawaii taxpayer identification number.
 - (iv) An individual's financial account number or credit or debit card number.
 - (v) A security code, access code, PIN, or password that would allow access to an individual's account.
 - (vi) Health insurance policy number, subscriber identification number, or any other unique number used by a health insurer to identify the person.
 - (vii) Medical history, medical treatment by a health-care professional, diagnosis of mental or physical condition by a health care professional, or deoxyribonucleic acid profile.
 - (viii) 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.
 - (ix) A digital signature or private key that is unique to an individual and that is used to authenticate or sign an electronic record.
- (2) "Business" shall have the same meaning as HRS 487-N.
- (3) "Consumer" means an individual residing in this State of Hawaii.
- (4) "Consumer Reporting Agency" shall have the same meaning as the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.)
- (5)(A) "Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the personal information of a consumer with whom the business does not have a direct relationship.
- (B) Examples of a direct relationship with a business include if the consumer is a past or present:
- (i) customer, client, subscriber, or user of the business's goods or services;
 - (ii) employee, contractor, or agent of the business;
 - (iii) investor in the business; or
 - (iv) donor to the business.

(C) The following activities conducted by a business, and the collection and sale or licensing of personal information incidental to conducting these activities, do not qualify the business as a data broker:

- (i) developing or maintaining third-party e-commerce or application platforms;
- (ii) providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier;
- (iii) providing publicly available information related to a consumer's business or profession; or
- (iv) providing publicly available information via real-time or near real-time alert services for health or safety purposes.

(D) The phrase "sells or licenses" does not include:

- (i) a one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; or
- (ii) a sale or license of data that is merely incidental to the business.

(6) "Security breach" shall have the same meaning as HRS 487-N.

(7) "License" means a grant of access to, or distribution of, data by one business to another in exchange for consideration. Sharing of data for the sole benefit of the business providing the data, where that business maintains sole control over the use of the data, is not a license.

(8) "Record" shall have the same meaning as HRS 487-N.

(9) "Request" means a request submitted by a consumer to a data broker for the purposes set forth in this act; and for which a data broker can reasonably verify, using commercially reasonable means, the authenticity of the request and the identity of the consumer.

DATA BROKERS ANNUAL REGISTRATION

(a) Annually, on or before January 31 following a year in which a business meets the definition of data broker, a data broker shall:

(1) register with the State of Hawaii's office of consumer protection;

(2) pay a registration fee of \$100.00; and

(3) provide the following information:

(A) the name and primary physical, e-mail, and Internet addresses of the data broker;

(B) The data broker's process that permits a consumer to opt out of the data broker's collection of personal information, opt out of its databases, or opt out of the sale of data:

(i) the method for requesting an opt-out;

(ii) if the opt-out applies to only certain activities or sales, which ones; and

(iii) whether the data broker permits a consumer to authorize a third party to perform the opt-out on the consumer's behalf;

(C) a statement specifying the data collection, databases, or sales activities from which a consumer may not opt out;

(D) a statement whether the data broker implements a purchaser credentialing process;

(E) the number of security breaches that the data broker has experienced during the prior year, and if known, the total number of consumers affected by the breaches;

(F) where the data broker has actual knowledge that it possesses the personal information of minors, a separate statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the personal information of minors; and

(G) any additional information or explanation the data broker chooses to provide concerning its data collection practices.

(b) The State of Hawaii's office of consumer protection shall create a page on its internet website where the information provided by data brokers under this title shall be accessible to the public.

(c) A data broker that fails to register is liable to the State for:

(1) a civil penalty of \$100.00 for each day it fails to register pursuant to this section;

(2) an amount equal to the fees due under this section during the period it failed to register pursuant to this section; and

(3) other penalties imposed by law and expenses incurred by the Attorney General in the investigation and prosecution of the action, as the court deems appropriate.

(d) The Attorney General may maintain an action in the Civil Division of the Superior Court to collect the penalties imposed in this section and to seek appropriate injunctive relief.

ACQUISITION, USE AND SALE OF PERSONAL INFORMATION; PROHIBITIONS

(a) Prohibited acquisition and use.

(1) A person shall not acquire personal information through fraudulent means.

(2) A person shall not acquire or use personal information for the purpose of:

(A) stalking or harassing another person;

(B) committing a fraud, including identity theft, financial fraud, or email fraud; or

(C) engaging in unlawful discrimination, including employment discrimination and housing discrimination.

(b) Sale.

(1) Any data broker, which is not a consumer reporting agency, shall establish a designated request process through which a consumer may submit a request pursuant to this section. A consumer may, at any time, submit a request through a designated request process to a data broker directing the data broker not to make any sale of any covered information the data broker has collected or will collect about the consumer.

(2) A data broker that has received a request submitted by a consumer shall not make any sale of any covered information the data broker has collected or will collect about that consumer. A data broker shall respond to a request submitted by a consumer within 60 days after receipt. A data broker may extend by not more than 30 days the period prescribed by this subsection if the operator determines that such an extension is reasonably necessary. An operator who extends the period prescribed by this subsection shall notify the consumer of such an extension.

DATA BROKER DUTY TO PROTECT INFORMATION;

(a) Duty to protect personal information.

(1) A data broker shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:

(A) the size, scope, and type of business of the data broker obligated to safeguard the personal information under such comprehensive information security program;

(B) the amount of resources available to the data broker;

(C) the amount of stored data; and

(D) the need for security and confidentiality of personal information.

(2) A data broker subject to this subsection shall adopt safeguards in the comprehensive security program that are consistent with the safeguards for protection of personal information and information of a similar character set forth in other State rules or federal regulations applicable to the data broker.

(b) Information security program; minimum features. A comprehensive information security program shall at minimum have the following features:

(1) designation of one or more employees to maintain the program;

(2) identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other records containing personal information, and a process for evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including:

(A) ongoing employee training, including training for temporary and contract employees;

(B) employee compliance with policies and procedures; and

(C) means for detecting and preventing security system failures;

(3) security policies for employees relating to the storage, access, and transportation of records containing personal information outside business premises;

(4) disciplinary measures for violations of the comprehensive information security program rules;

(5) measures that prevent terminated employees from accessing records containing personal information;

(6) supervision of service providers, by:

(A) taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information consistent with applicable law; and

(B) requiring third-party service providers by contract to implement and maintain appropriate security measures for personal information;

(7) reasonable restrictions upon physical access to records containing personal information and storage of the records and data in locked facilities, storage areas, or containers;

(8)(A) regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and

(B) upgrading information safeguards as necessary to limit risks;

(9) regular review of the scope of the security measures:

(A) at least annually; or

(B) whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information; and

(10)(A) documentation of responsive actions taken in connection with any incident involving a breach of security; and

(B) mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

(c) Information security program; computer system security requirements. A comprehensive information security program required by this section shall at minimum, and to the extent technically feasible, have the following elements:

(1) secure user authentication protocols, as follows:

(A) an authentication protocol that has the following features:

(i) control of user IDs and other identifiers;

- (ii) a reasonably secure method of assigning and selecting passwords or use of unique identifier technologies, such as biometrics or token devices;
 - (iii) control of data security passwords to ensure that such passwords are kept in a location and format that do not compromise the security of the data they protect;
 - (iv) restricting access to only active users and active user accounts; and
 - (v) blocking access to user identification after multiple unsuccessful attempts to gain access; or
 - (B) an authentication protocol that provides a higher level of security than the features specified in subdivision (A) of this subdivision (c)(1).
- (2) secure access control measures that:
- (A) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
 - (B) assign to each person with computer access unique identifications plus passwords, which are not vendor-supplied default passwords, that are reasonably designed to maintain the integrity of the security of the access controls or a protocol that provides a higher degree of security;
- (3) encryption of all transmitted records and files containing personal information that will travel across public networks and encryption of all data containing personal information to be transmitted wirelessly or a protocol that provides a higher degree of security;
- (4) reasonable monitoring of systems for unauthorized use of or access to personal information;
- (5) encryption of all personal information stored on laptops or other portable devices or a protocol that provides a higher degree of security;
- (6) for files containing personal information on a system that is connected to the Internet, reasonably up-to-date firewall protection and operating system security patches that are reasonably designed to maintain the integrity of the personal information or a protocol that provides a higher degree of security;
- (7) reasonably up-to-date versions of system security agent software that must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions and is set to receive the most current security updates on a regular basis or a protocol that provides a higher degree of security; and
- (8) education and training of employees on the proper use of the computer security system and the importance of personal information security.

DISCLOSURES TO CONSUMERS

- (a) A data broker shall, upon verified request of any consumer, clearly and accurately disclose to the consumer all information that the data broker has collected at the time of the request pertaining to the consumer, including:
- (1) the categories of personal information it has shared about that consumer.
 - (2) the categories of sources from which the personal information is collected.
 - (3) the names of third parties with whom the data broker has shared personal information during the prior 12-month period and the date of each request;
 - (4) the specific pieces of personal information it has shared about that consumer.
- (c) A data broker may provide disclosure to a consumer at any time, but shall not be required to provide disclosure to a consumer more than twice in a 12-month period.
- (d) Additionally, consumer reporting agencies that broker data of residents of the State of Hawaii shall annually provide a written notice to consumers, in at least 12 point type, containing the following information;

- (1) under what circumstances the consumer’s has the right to receive a free copy of their credit report and the methods for obtaining the report;
- (2) under what circumstances a person may access a consumer’s credit report without their permission, such as in response to a court order; for direct mail offers of credit;
- (3) an explanation of a security freeze, along with what circumstances the consumer has the right to place a “security freeze” on a credit report, and the costs and process for placing the freeze; and
- (4) notice that if the consumer believes a law regulating consumer credit reporting has been violated, they may file a complaint with the Federal Trade Commission, with the processes for filing the complaint.

ENFORCEMENT.

- (a) A person or business who violates a provision of this act commits an unfair and deceptive act in commerce of [INSERT REFERENCE].
- (b) The Attorney General has the same authority to adopt rules to implement the provisions of this section and to conduct civil investigations, enter into assurances of discontinuance, bring civil actions, and take other enforcement actions as provided under this title.

Nov. 15 meeting – list of current bills

All bills define a data broker as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship

CA AB 1202	Signed by Governor	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. Has a carve out for consumer reporting agencies, financial institutions covered under GLBA, and companies covered by CA’s Insurance Information and Privacy Protection Act
IL HB 2871	Pending	Creates the Data Broker Registration Act, requires a data broker to annually register with the secretary of state, defines data broker as a business or unit of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.
ND HB 1524	Failed	Relates to the regulation of data brokers, provides a penalty.
VT H.764	Enacted	Requires data brokers to register with the attorney general. “Data brokers also must disclose annually their practices, if any, for allowing consumers to opt out. Also requires data brokers to have an Information Security Program. Further, the law requires data brokers to report annually

the number of data breaches experienced during the prior year and, if known the total number of consumers affected by the breaches.”

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.

Enforcement is by the state Attorney General with fines up to \$10,000 per year for failure to register.

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.

Vermont has a carve out for state agencies.

154 data brokers have registered (as of 11/14/19)

<https://www.vtsosonline.com/online/DataBrokerInquire/DataBrokerSearch>

Geolocation Data

Proposal

A BILL FOR AN ACT

RELATING TO GEOLOCATION PRIVACY PROTECTION

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

SECTION 1. The legislature finds that technology is rapidly evolving, often faster than society is aware. One increasingly widespread technology application is the use of geolocation data generated by mobile devices and application software. These devices include smartphones, tablets, personal computers, vehicles, and smartwatches. The applications are varied, including maps, browsers, cameras, social media, and sometimes even unexpected applications such as flashlights.

The legislature further finds that three in every four people in the United States have a smartphone, which are usually equipped to collect geolocation information. Certain companies have been found to record, collect, and preserve geolocation data. When geolocation data is collected from a smartphone or other device that people tend to keep on or near their person, the geolocation data essentially becomes a permanent record of a person's movement and daily life.

The legislature further finds that in recent years, companies that record, collect, and preserve geolocation data

have sold this data, often without the knowledge or consent of the person who is the primary user of the device or application. The legislature acknowledges that the sale or offering for sale of geolocation data, which is essentially a permanent record of a person's movement and daily life, without the person's knowledge or consent, is an unfair and deceptive practice.

Accordingly, the purpose of this Act is to prohibit the sale or offering for sale of geolocation data without the explicit consent of the individual who has primary use of the device or application.

SECTION 2. DEFINITIONS

"Geolocation information" means information that: (i) is not the contents of a communication; (ii) is generated by or derived from, in whole or in part, the operation of a mobile device, including, but not limited to, a smart phone, tablet, or laptop computer; and (iii) is sufficient to determine or infer the precise location of that device. "Geolocation information" does not include Internet protocol addresses.

"Location-based application" means a software application that is downloaded or installed onto a device and collects, uses, or stores geolocation information.

"User" means a person who purchases or leases a device or installs or uses an application.

SECTION 3. Chapter 481B, Hawaii Revised Statutes, is amended by adding a new section to part I to be appropriately designated and to read as follows:

"§481B- Sale of geolocation data without consent is prohibited. (a) No person shall sell or offer for sale geolocation data that is recorded or collected by mobile devices or location-based applications without the explicit consent of the individual who is the primary user of the device or application.

SECTION 4. This Act does not affect rights and duties that matured, penalties that were incurred, and proceedings that were begun before its effective date.

SECTION 5. New statutory material is underscored.

SECTION 6. This Act shall take effect on July 1, 2020.

Report Title:

Geolocation Privacy; Unfair and Deceptive Practices; Geolocation Data

Description:

Prohibits the sale or offering for sale of geolocation data collected using mobile devices or location-based applications without the explicit consent of the individual who is the primary user of the device or application.

Nov. 15 meeting – list of current bills

CA AB 523	Pending	Prescribes the circumstances under which telephone and telegraph corporations may release specified information, including customer proprietary network information, regarding noncommercial subscribers without their written consent. Specifically includes geolocation information in the information that may only be released with a noncommercial subscriber's written consent.
CA Ballot initiative	2020	California Consumer Privacy Rights and Enforcement Act of 2020 Creates a concept of sensitive personal information that includes precise geolocation data. "Precise geolocation" means any data that locates a consumer within a geographic area that is equal to or less than the area of a circle with a radius of half of one mile.
CT SB 432	Failed	Expands unfair trade practices to include sale of a customer's global positioning system (GPS) location by mobile phone providers, protects the privacy of mobile telephone users.
HI HB 702	Vetoed	Prohibits the sale or offering for sale of location data collected using satellite navigation technology without the explicit consent of the individual who is the primary user of the satellite navigation technology equipped device.
IL HB 2785	Pending	Creates the Geolocation Privacy Protection Act, defines geolocation information, location-based application, private entity, and user, provides that a private entity may not collect, use, store, or disclose geolocation information from a location-based application on a user's device unless the private entity first receives the person's affirmative express consent after complying with specified notice requirements, provides exceptions, provides that a violation of the act constitutes an unlawful practice.
KY SB 243	Failed	Prohibits telecommunications companies from disclosing or transmitting to a third party any location data derived from a cellular phone without the consent of the customer.
NJ AB 4974 SB 3497	Pending	Requires operators of mobile device applications that collect user global positioning system data to notify users about how global positioning system data is disclosed and allow users to opt in to disclosure.
NYC Int 1632- 2019	Pending	Prohibits telecommunications carriers and mobile applications from sharing a user's location data, if the location is within NYC. This bill would also prohibit anyone who receives such location data from sharing it with another person. The penalty would be \$1,000 per violation, with a maximum \$10,000 per day per person whose location data was unlawfully shared. The Dept. of IT and Telecommunications would enforce. This bill would also create a private right of action.
SC HB 3701	Pending	Enacts the state Cellular Data Privacy Protection Act, defines relevant terms, prohibits a mobile telecommunications provider from selling a customer's personal data to a third party, imposes a penalty, authorizes the attorney general to investigate and enforce alleged violations of this act.

A BILL FOR AN ACT

RELATING TO _____.

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

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

4 §803-41 Definitions. As used in this part, unless the
5 context clearly requires otherwise:

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

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

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

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

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

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

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

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

- 20 (1) Any wire or oral communication;
- 21 (2) Any communication made through a tone-only paging
22 device;
- 23 (3) Any communication from a tracking device; or
- 24 (4) Electronic funds transfer information stored by [a]
25 financial institution in a communications system used for the
26 electronic storage and transfer of funds.

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

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

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

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

14 (A) Furnished to the subscriber or user by a provider
15 of wire or electronic communication service in the ordinary
16 course of its business and being used by the subscriber or user
17 in the ordinary course of its business or furnished by the
18 subscriber or user for connection to the facilities of the
19 services and used in the ordinary course of its business; or

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

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

26 "Electronic storage" means:

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

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

7 "Electronically stored data" means any information that is
8 recorded, stored, or maintained in electronic form by an
9 electronic communication service or a remote computing service,
10 and includes, but is not limited to, the contents of
11 communications, transactional records about communications, and
12 records and information that relate to a subscriber, customer,
13 or user of an electronic communication service or a remote
14 computing service.

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

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

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

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

3 "Pen register" means a device that records or decodes
4 electronic or other impulses that identify the numbers dialed or
5 otherwise transmitted on the telephone line or cellular network
6 to which the device is connected, or that identifies the numbers
7 that a device uses to connect to a wire or electronic
8 communications service, but the term does not include any device
9 used by a provider or customer of a wire or electronic
10 communication service for billing, or recording as an incident
11 to billing, for communication services provided by the provider
12 or any device used by a provider or customer of a wire
13 communication service for cost accounting or other similar
14 purposes in the ordinary course of its business.

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

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

21 (1) Scrambled or encrypted;

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

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

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

4 (5) Transmitted on frequencies allocated under part 25,
5 subpart D, E, or F of part 74, or part 94 of the Rules of the
6 Federal Communications Commission, unless in the case of a
7 communication transmitted on a frequency allocated under part 74
8 that is not exclusively allocated to broadcast auxiliary
9 services, the communication is a two-way voice communication by
10 radio.

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

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

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

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

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

1 "User" means any person or entity that:

2 (1) Uses an electronic communication service; and

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

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

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

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

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

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

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

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

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

21 ~~— (2) A provider of electronic communication service or~~
22 ~~remote computing service shall disclose a record or other~~
23 ~~information pertaining to a subscriber to, or customer of, the~~
24 ~~service (other than the contents of an electronic communication)~~
25 ~~to a governmental entity only when:~~

26 ~~— (A) Presented with a search warrant;~~

1 ~~————— (B) Presented with a court order, which seeks the~~
2 ~~disclosure of transactional records, other than real-time~~
3 ~~transactional records;~~

4 ~~————— (C) The consent of the subscriber or customer to the~~
5 ~~disclosure has been obtained; or~~

6 ~~————— (D) Presented with an administrative subpoena~~
7 ~~authorized by statute, an attorney general subpoena, or a grand~~
8 ~~jury or trial subpoena, which seeks the disclosure of~~
9 ~~information concerning electronic communication, including but~~
10 ~~not limited to the name, address, local and long distance~~
11 ~~telephone billing records, telephone number or other subscriber~~
12 ~~number or identity, and length of service of a subscriber to or~~
13 ~~customer of the service, and the types of services the~~
14 ~~subscriber or customer utilized.]~~

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

19 ~~[(e) A court order for disclosure under subsection (d)~~
20 ~~shall issue only if the governmental entity demonstrates~~
21 ~~probable cause that the records or other information sought,~~
22 ~~constitute or relate to the fruits, implements, or existence of~~
23 ~~a crime or are relevant to a legitimate law enforcement inquiry.~~
24 ~~An order may be quashed or modified if, upon a motion promptly~~
25 ~~made, the service provider shows that compliance would be unduly~~
26 ~~burdensome because of the voluminous nature of the information~~

1 ~~or records requested, or some other stated reason establishing~~
2 ~~such a hardship.]~~

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

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

17 SECTION 3. Chapter 803, Hawaii Revised Statutes, is
18 amended to read as follows:

19 §803-47.7 Backup preservation. (a) A governmental entity
20 may include in its [~~court order~~] search warrant a requirement
21 that the service provider create a backup copy of the contents
22 of the electronic communication without notifying the subscriber
23 or customer. The service provider shall create the backup copy
24 as soon as practicable, consistent with its regular business
25 practices, and shall confirm to the governmental entity that the
26 backup copy has been made. The backup copy shall be created

1 within two business days after receipt by the service provider
2 of the subpoena or court order.

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

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

9 (1) The delivery of the information; or

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

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

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

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

21 (e) Within fourteen days after notice by the governmental
22 entity to the subscriber or customer under subsection (b) of
23 this section, the subscriber or customer may file a motion to
24 vacate the [~~court order~~] search warrant, with written notice and
25 a copy of the motion being served on both the governmental
26 entity and the service provider. The motion to vacate a [~~court~~

1 ~~order~~] search warrant shall be filed with the designated judge
2 who issued the [~~order~~] warrant. The motion or application shall
3 contain an affidavit or sworn statement:

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

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

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

21 (g) If the court finds that the applicant is not the
22 subscriber or customer whose communications are sought, or that
23 there is reason to believe that the law enforcement inquiry is
24 legitimate and the justification for the communications sought
25 is supported by probable cause, the application or motion shall
26 be denied, and the court shall order the release of the backup

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

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

11 §803-47.8 Delay of notification. (a) A governmental
12 entity may as part of a request for a [~~court order~~] search
13 warrant include a provision that notification be delayed for a
14 period not exceeding ninety days or, at the discretion of the
15 court, no later than the deadline to provide discovery in a
16 criminal case, if the court determines that notification of the
17 existence of the court order may have an adverse result.

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

- 20 (1) Endangering the life or physical safety of an
21 individual;
- 22 (2) Flight from prosecution;
- 23 (3) Destruction of or tampering with evidence;
- 24 (4) Intimidation of a potential witness; or
- 25 (5) Otherwise seriously jeopardizing an investigation or
26 unduly delaying a trial.

1 (c) Extensions of delays in notification may be granted up
2 to ninety days per application to a court or, at the discretion
3 of the court, up to the deadline to provide discovery in a
4 criminal case. Each application for an extension must comply
5 with subsection (e) of this section.

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

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

12 (2) Informs the customer or subscriber:

13 (A) Information maintained for the customer or
14 subscriber by the service provider or request was supplied to or
15 requested by that governmental authority and the date on which
16 the supplying or request took place;

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

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

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

24 (e) A governmental entity may apply to the designated
25 judge or any other circuit judge or district court judge, if a
26 circuit court judge has not yet been designated by the chief

1 justice of the Hawaii supreme court, or is otherwise
2 unavailable, for an order commanding a provider of an electronic
3 communication service or remote computing service to whom a
4 search warrant, or court order is directed, not to notify any
5 other person of the existence of the search warrant [~~, or court~~
6 ~~order~~] for such period as the court deems appropriate not to
7 exceed ninety days or, at the discretion of the court, no later
8 than the deadline to provide discovery in a criminal case. The
9 court shall enter the order if it determines that there is
10 reason to believe that notification of the existence of the
11 search warrant [~~, or court order~~] will result in:

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

19 SECTION 5. This Act does not affect rights and duties that
20 matured, penalties that were incurred, and proceedings that were
21 begun before its effective date.

22 SECTION 6. Statutory material to be repealed is bracketed
23 and stricken. New statutory material is underscored.

24 SECTION 7. This Act shall take effect upon approval.

25

INTRODUCED BY: _____

Report Title:

RELATING TO VIOLATION OF PRIVACY

Description:

Amends the offense of violation of privacy in the first degree to include scenarios involving the creation and dissemination of "deep fake" images and videos that use the recognizable physical characteristics of a known person to create a fictitious person depicted in the nude or engaging in sexual conduct.

A BILL FOR AN ACT

RELATING TO VIOLATION OF PRIVACY.

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

1 SECTION 1. Section 711-1110.9, Hawai'i Revised Statutes,
2 is amended to read as follows:

3 "§711-1110.9 Violation of privacy in the first degree.

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

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

13 (b) the person knowingly discloses or threatens to
14 disclose an image or video of another identifiable person either
15 in the nude, as defined in section 712-1210, or engaging in
16 sexual conduct, as defined in section 712-1210, without the
17 consent of the depicted person, with intent to harm
18 substantially the depicted person with respect to that person's

____. B. NO.

1 health, safety, business, calling, career, education, financial
2 condition, reputation, or personal relationships or as an act of
3 revenge or retribution; [~~provided that:~~] or

4 (c) the person intentionally creates or discloses, or
5 threatens to disclose, an image or video of a fictitious person
6 depicted in the nude, as defined in section 712-1210, or engaged
7 in sexual conduct, as defined in section 712-1210, that includes
8 the recognizable physical characteristics of a known person such
9 that the image or video appears to depict the known person and
10 not a fictitious person, with intent to harm substantially the
11 depicted person with respect to that person's health, safety,
12 business, calling, career, education, financial condition,
13 reputation, or personal relationships, or as an act of revenge
14 or retribution.

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

17 (A) When the person was voluntarily nude in public or
18 voluntarily engaging in sexual conduct in public; or

19 (B) Pursuant to a voluntary commercial transaction. ~~†~~
20 ~~and]~~

____. B. NO.

1 (3) [~~(1)~~] Nothing in this [~~paragraph~~] section shall be
2 construed to impose liability on a provider of "electronic
3 communication service" or "remote computing service" as those
4 terms are defined in section 803-41, for an image or video
5 disclosed through the electronic communication service or remote
6 computing service by another person.

7 (4) [~~(2)~~] Violation of privacy in the first degree is a
8 class C felony. In addition to any penalties the court may
9 impose, the court may order the destruction of any recording
10 made in violation of this section.

11 (5) [~~(3)~~] Any recording or image made or disclosed in
12 violation of this section and not destroyed pursuant to
13 subsection [~~(2)~~] (4) shall be sealed and remain confidential.

14 SECTION 3. Statutory material to be repealed is bracketed
15 and stricken. New statutory material is underscored

16 SECTION 4. This Act shall take effect upon approval.

INTRODUCED BY: _____

Report Title:

RELATING TO VIOLATION OF PRIVACY

Description:

Amends the offense of violation of privacy in the first degree to include scenarios involving the creation and dissemination of "deep fake" images and videos that use the recognizable physical characteristics of a known person to create a fictitious person depicted in the nude or engaging in sexual conduct.

A BILL FOR AN ACT

RELATING TO VIOLATION OF PRIVACY.

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

1 SECTION 1. Section 711-1110.9, Hawai'i Revised Statutes,
2 is amended to read as follows:

3 "§711-1110.9 Violation of privacy in the first degree.

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

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

13 (b) the person knowingly discloses or threatens to
14 disclose an image or video of another identifiable person either
15 in the nude, as defined in section 712-1210, or engaging in
16 sexual conduct, as defined in section 712-1210, without the
17 consent of the depicted person, with intent to harm
18 substantially the depicted person with respect to that person's

____. B. NO.

1 health, safety, business, calling, career, education, financial
2 condition, reputation, or personal relationships or as an act of
3 revenge or retribution; [~~provided that:~~] or

4 (c) the person intentionally creates or discloses, or
5 threatens to disclose, an ~~image or~~ **digitally altered** video of a
6 ~~fictitious person that~~ depicts a **known person** in the nude, as
7 defined in section 712-1210, or engaged in sexual conduct, as
8 defined in section 712-1210, that includes the recognizable
9 physical characteristics of a known person such that the ~~image~~
10 ~~or~~ video appears to depict the known person and not a fictitious
11 person **in the nude or engaged in sexual conduct that the**
12 **individual did not actually perform,** with intent to harm
13 substantially the depicted person with respect to that person's
14 health, safety, business, calling, career, education, financial
15 condition, reputation, or personal relationships, or as an act
16 of revenge or retribution.

17 (2) [~~(i)~~] This [~~paragraph~~] section shall not apply to

18 images or videos of the depicted person made:

19 (A) When the person was voluntarily nude in public or

20 voluntarily engaging in sexual conduct in public; or

____. B. NO.

1 (B) Pursuant to a voluntary commercial transaction. ~~†~~
2 and]

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

9 (4) [~~(2)~~] Violation of privacy in the first degree is a
10 class C felony. In addition to any penalties the court may
11 impose, the court may order the destruction of any recording
12 made in violation of this section.

13 (5) [~~(3)~~] Any recording or image made or disclosed in
14 violation of this section and not destroyed pursuant to
15 subsection [~~(2)~~] (4) shall be sealed and remain confidential.

16 SECTION 3. Statutory material to be repealed is bracketed
17 and stricken. New statutory material is underscored

18 SECTION 4. This Act shall take effect upon approval.

INTRODUCED BY: _____

Dear Committee Members:

My name is Oren T. Chikamoto. I am the retained counsel and lobbyist for the American Council of Life Insurers (ACLI) in the State of Hawaii.

ACLI advocates on behalf of 280 member companies dedicated to providing products and services that promote consumers' financial and retirement security. 90 million American families depend on our members for life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, dental and vision and other supplemental benefits. ACLI represents member companies in state, federal and international forums for public policy that supports the industry marketplace and the families that rely on life insurers' products for peace of mind. ACLI members represent 95 percent of industry assets in the United States. Two hundred twenty-one (221) ACLI member companies currently do business in the State of Hawaii; and they represent 95% of the life insurance premiums and 99% of the annuity considerations in this State.

As respects financial institutions such as life and other insurers, two fundamental concepts should be considered by the Committee in the formulation of new laws relating to privacy:

- Any new law should be harmonized with existing privacy laws and regulations and while this harmonization occurs businesses in the financial services industry, such as life and other insurers, should be exempted, just as they are under CCPA. I've provided some Hawaii specific exemption language below.
- Any new law should give companies an appropriate amount of time to come into compliance. Preferably 2 years like the E.U. GDPR.

Suggested Financial Services Exemption:

"Nothing in [PROPOSED STATUTE] shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution subject to, or personal information collected, used or disclosed pursuant to, the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the Privacy of Consumer Financial Information as provided in Hawaii's Insurance Code (HI Rev. Stat. Ann. §431:3A-101. et seq.).

[PROPOSED STATUTE] shall not apply to a covered entity subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5)."

Rationale for the exemption:

The Gramm-Leach-Bliley Act (GLBA) is a federal law that requires financial institutions to maintain consumer privacy protections and regulates how those institutions may disclose certain consumer information to non-affiliated third parties. GLBA is an established and comprehensive federal privacy law that provides protections for consumers, and companies in compliance with GLBA should be completely exempt from the requirements imposed by Senate Bill 418. The inclusion of this exemption is

necessary to ensure the proper functioning of existing privacy laws for Hawaii public and private entities that rely on this information. Due to the completeness of this federal oversight scheme, many state data breach notice laws already exempt financial institutions subject to the GLBA. This same rationale and scheme applies to companies which must comply with HIPAA and HITECH, the federal comprehensive and primary health care data privacy statutes.

In addition, Privacy of Consumer Financial statutes as provided in Hawaii's Insurance Code (such as HRS §431:3A-101. et seq.). already regulates the collection, use and disclosure of nonpublic personal information gathered about individuals by all insurance licensees. This rule:

- (1) Requires licensees to provide notice to individuals about its privacy policies and practices;
- (2) Establishes the conditions under which a licensee may disclose nonpublic personal financial information about individuals to affiliates and nonaffiliated third parties; and
- (3) Provides methods for individuals to prevent a licensee from disclosing that information.

Financial institutions operating in Hawaii are governed by a comprehensive framework for the protection of personal information: <https://members.acli.com/-/media/ACLI/Members/Files/Compliance/Compliance-Services/Privacy/18PVHI.ashx?la=en>

Expanded Private Cause of Action:

Lastly while the changes the Committee is proposing to the private right of action do not directly impact the life insurance industry we oppose any further expansion of this provision. As represented by our statutes above and in many other areas of Hawaii law, there is comprehensive and meaningful regulatory obligation on businesses, especially, insurers to protect consumer privacy. There is also strict regulatory enforcement provisions that adequately arm state officials for any action needed against bad actors. Private causes of action are clogging Hawaii courts and provide no real benefit to Hawaii consumers. Applicable State agencies, such as Hawaii's Insurance Division and the State's Department of Commerce and Consumer Affairs, generally, which are the functional regulators in the business sector provide far stronger, far faster outcomes and greater deterrence than the court system can currently provide.

Thank you for your thoughtful consideration of my client's concerns.

Sincerely, Oren.

Oren T. Chikamoto. Esq.
Law Offices of Oren T. Chikamoto
A Limited Liability Law Company
1001 Bishop Street, Suite 1750
American Savings Bank Tower
Honolulu, Hawaii 96813
Tel: (808) 531--1500
E Mail: otc@chikamotolaw.com

Aloha Senator Kidani, Representative Lee, and members of the 21 Century Privacy Task Force,

I'm writing to follow up on the question posed to HIDOE at the 11/15/18 21 Century Privacy Task Force meeting, about whether or not HIDOE has required courses or established curriculum that addresses privacy training or privacy awareness to the general student population. There is no established curriculum or course work that addresses privacy training or privacy awareness to the general student population. However, some advisory information is being disseminated through various Computer Science media courses. Additionally, OCID has been going out with a presentation to teachers on Digital Literacy that incorporates information on online awareness and safety. They reference HIDOE's "Internet Safety" webpage as an additional resource.

Here is more detailed information from OCID:

Privacy Awareness and Training is part of our [K-12 Computer Science Standards](#) Impacts of Computing concept area. For this area, we have been recommending the free K-12 Digital Citizenship curriculum from [Common Sense Education](#) that covers:

- *Media Balance & Well-Being*
- *Privacy & Security*
- *Digital Footprint & Identity*
- *Relationships & Communication*
- *Cyberbullying, Digital Drama & Hate Speech*
- *News & Media Literacy*

In addition, there are some related websites that we added to the HIDOE's [Internet Safety](#) website to supplement the Common Sense Education curriculum resource:

- [Hawaii Internet Crimes Against Children Task Force](#)
- [NetSmartz Workshop: Basic Internet Safety](#)
- [Kids Health: Internet Safety](#)
- [Stay Safe Online](#)

*We are just starting to work with our Complex Area Computer Science Support Teams on their **School Design for Computer Science** plan that covers the Privacy along the rest of the five (5) main concept areas from the [K-12 Computer Science Framework](#):*

1. *Computing Systems*
2. *Networks and the Internet*
3. *Data and Analysis*
4. *Algorithms and Programming*
5. *Impacts of Computing*

-Jessica Honbo,
Student Information and Privacy, Information Specialist
State of Hawaii, Department of Education
Office of Strategy, Innovation and Performance
Data Governance and Analysis Branch