	Referred to as	Effective Date	Covered Individuals	Scope (Who does it apply to?)	Enforced By	Private Right of Action	Do Not Sell Requirement	Right to Access	Right of Deletion	Prohibition of Discrimination	Right to Opt-Out	Opt-In (Age)	Right of Portability	Data Breach Notification
California	*California Consumer Privacy Act (CCPA)* [AB 375/ SB 1211]	Jan. 1, 2020	California Residents	Businesses, Service Providers	AG (until Privacy Agency takeover)	Yes	Yes	Yes	Yes	Yes	Yes	Yes (16)	Yes	No (addressed elsewhere)
	California Privacy Rights Act (CPRA)	Jan. 1, 2023	California Residents	Businesses, Service Providers, Third Parties	Privacy Agency	Yes	Yes	Yes	Yes	Yes	Yes	Yes (16)	Yes	No (addressed in other CA law)
Colorado	Colorado Protections for Consumer Data Privacy Act C.R.S. § 6-1-716	Sept. 1, 2018	Colorado Residents	"Covered Entity"[1]	AG	No	No	No	No	No	No	No	No	No
Florida (Proposed)	CS/HB 969	Proposed	Florida consumers – i.e., those who reside or are domiciled	Certain businesses that collect PI and pass certain thresholds	AG	Yes	Yes	Yes	Yes	Yes	Yes	Yes (13-15)	Yes	No
Maine	*An Act to Protect the Privacy of Online Consumer Information* [LD 946]	July 1, 2020	An applicant for or a current or former subscriber of broadband Internet access service.	Providers of broadband internet services	Public Utilities Commission (ME ST T. 35-A § 1508-A)	No	Yes	No	No	No	Opt-in	Yes (18)[2]	No	No

[1] "Covered entity" means a Person, defined as an "an individual, corporation, business trust, estate, trust, partnership, unincorporated association, or two or more thereof having a joint or common interest, or any other legal or commercial entity," that maintains, owns, or licenses personal information in the course of the person's business, vocation, or occupation. (C.R.S. § 6-1-176). "Covered entity" does not include a person acting as a third-party service provider.

[2] 18 years of age is identified as the default likely needed to enter into the underlying contract with the broadband provider.

	Referred to as	Effective Date	Covered Individuals	Scope (Who does it apply to?)	Enforced By	Private Right of Action	Do Not Sell Requirement	Right to Access	Right of Deletion	Prohibition of Discrimination	Right to Opt-Out	Opt-In (Age)	Right of Portability	Data Breach Notification
Minnesota (Proposed)	*Minnesota Consumer Data Privacy Act (MCDPA) [HF 1492]*	June 30, 2022	"Consumers"	"Businesses"	AG	No	Yes	Yes	Yes	Yes	Yes	No	Yes	No (Addressed in another MN law)
Nevada	*Nevada Privacy of Information Collected On Internet From Consumers (NPICIC)* [SB 220/ Ch. 603A]	Oct. 1, 2019	"Consumer"	"Operator"	AG	No	No	No	No	No	Yes	No	No	No
New York	*Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)* [S5575B]	March 21, 2020	NY Residents	"Covered Entity"	AG	No	No	No	No	No	No	No	No	Yes
Oklahoma	*Oklahoma Computer Data Privacy Act (OCDPA)*[3] [HB1602]	Jan. 1, 2023	"Consumers"	"Business" (for-profit entities)	AG	No	Yes	Yes	Yes	Yes	Yes	No	No	No
Utah (Proposed)	*Utah Consumer Privacy Act [S.B. 200]*	Jan. 1, 2022	"Consumers"	Certain businesses that collect PI and pass certain thresholds	AG	No	Yes	Yes	Yes	Yes	Yes	No	Yes	No

[3] OCDPA has found that the strictly "opt-out" of data processing approach used by other states such as California and Virginia are "ineffectual and poses an immediate risk to the health, safety and welfare of individuals within Oklahoma." Therefore, if passed, businesses will be required to collect opt-in consent from consumers prior to processing their personal information.

	Referred to as	Effective Date	Covered Individuals	Scope (Who does it apply to?)	Enforced By	Private Right of Action	Do Not Sell Requirement	Right to Access	Right of Deletion	Prohibition of Discrimination	Right to Opt-Out	Opt-In (Age)	Right of Portability	Data Breach Notification
Vermont	*Vermont's Security Breach Notice Act*[4] [Bill S.110]	July 1, 2020	"Consumers"	"Business" (commercial entity) & "Data Collector"	AG, State's Attorney & Department of Financial Regulation	No	Not included	Not included	Not included	Not included	Not included	Not included	Not included	✓
Virginia	*Virginia Consumer Data Protection Act (VCDPA)* [SB1392/HB2307]	Jan. 1, 2023	"Consumers"[5]	Persons that conduct business in Virginia[6]	AG	No	Yes[7]	Yes	Yes	Yes	Yes	Yes (For Sensitive Data)	Yes	Yes
Washington	*SSB-5062*	July 31, 2022	Washington Residents	Persons that conduct business in Washington or produce products or services that are targeted to residents of Washington.	AG	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes

4 The Vermont Security Breach Notice Act went into effect July 1, 2020 and amended the pre-existing privacy statute including the definition of PII, an alternate notification process for login credentials, and a change to substitute notice requirements. This also enacted a separate "Student Online Personal Information Protection Act" like the one in CA and 20 other states.

5 Defined as "a natural person who is a resident of the Commonwealth acting *only* in an individual or household context." Excludes: a natural person acting in a commercial or employment context.

6 The Virginia Consumer Data Protection Act recites: "This chapter applies to persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that (i) during a calendar year, control or process personal data of at least 100,000 consumers or (ii) control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data."

7 Consumers have the right to opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects.

California	
California Consumer Privacy Act [Ca. Civ. Code 1798.100, *et seq.*]	
Definition of "***personal info***"	"Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household: (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers. (B) Any categories of personal information described in subdivision (e) of Section 1798.80. (C) Characteristics of protected classifications under California or federal law. (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies. (E) Biometric information. (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement. (G) Geolocation data. (H) Audio, electronic, visual, thermal, olfactory, or similar information. (I) Professional or employment-related information. (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99). (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

	(2) “Personal information” does not include publicly available information. For purposes of this paragraph, “publicly available” means information that is lawfully made available from federal, state, or local government records. “Publicly available” does not mean biometric information collected by a business about a consumer without the consumer’s knowledge. (3) “Personal information” does not include consumer information that is deidentified or aggregate consumer information.
Definition of “***business***”	“Business” means: (1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers’ personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information, that does business in the State of California, and that satisfies one or more of the following thresholds: (A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185. (B) Alone or in combination, annually buys, receives for the business’ commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices. (C) Derives 50 percent or more of its annual revenues from selling consumers’ personal information. (2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business. “Control” or “controlled” means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. “Common branding” means a shared name, servicemark, or trademark.
Data Breach Notification	Data Breach notification is not addressed under CCPA. CCPA does, however, establish a 30-day “cure” period before a private right of action may be commenced and imposes statutory damages for data breaches in the amount of “less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.”
Definition of “service provider”	“Service provider” means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.
Definition of “consumer”	A California resident.
Enforcement	Attorney General (and subsequently a newly established Privacy Agency). $2,500 fine per violation or up to $7,500 per violations if such violations are intentional.

Colorado	
Colorado Protections for Consumer Data Privacy Act (CDPA) [C.R.S. § 6-1-716]	
Definition of "***covered information***"	Covered information includes Personal Identifying Information and Personal Information. Personal Identifying Information includes social security numbers; personal identification numbers; passwords; pass codes; official state or government-issued driver's license or identification card numbers; government passport numbers; biometric data; employer, student, or military identification numbers; and financial transaction devices, including financial account numbers. Personal Information includes a Colorado resident's first name or first initial and last name in combination with any of the following: 1. Social Security number; 2. Driver's license number or identification card number 3. Student, military, or passport identification number; 4. Medical information 5. Health insurance identification number; or 6. Biometric data used to authenticate an individual when they access an online account. Personal information also includes a Colorado resident's username or e-mail address, in combination with a password or security questions and answers that would permit access to an online account; and A Colorado resident's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.
Definition of "***covered entity***"	A person, commercial entity, or governmental entity who: 1. Maintains, own or licenses personal information in the course of the person's business, vocation, or occupation Covered Entity does not include a person acting as a third party service provider.
When to notify Colorado residents of a security breach.	Once the Covered Entity becomes aware that a security breach may have occurred, the Covered entity must conduct a prompt investigation and provide notice to affected Colorado residents. Covered Entity has 30 days to provider notice after the date of determination that a security breach has occurred.
Enforcement	Attorney General $2,500 fine per violation or up to $7,500 per violations if such violations are intentional.

Florida (proposed)	
House Bill 969	
Scope	The proposed bill applies to controllers that collect personal information about consumers.
Definition of "***personal information***"	Personal information means information that identifies, relates to, or describes a consumer or household, or is reasonably capable of being directly or indirectly associated or linked with, a consumer or household. The term includes, but is not limited to, the following: 1. Identifiers such as real name, alias, postal address, unique identifier, online identifier, internet protocol address, email address, account name, social security number, driver license number, passport number, or other similar identifiers. 2. Information that identifies, relates to, or describes, or could be associated with, a particular individual. 3. Characteristics of protected classifications under state or federal law. 4. Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies. 5. Biometric information. 6. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet website, application, or advertisement. 7. Geolocation data. 8. Audio, electronic, visual, thermal, olfactory, or similar information. 9. Inferences drawn from any of the information identified in this paragraph to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. There are a number of exceptions, including deidentified or aggregate consumer information and publicly available information.
Definition of "***controller***"	Controller means a sole proprietorship, partnership, limited liability company, corporation, association, or legal entity that meets the following requirements: 1. Is organized or operated for the profit or financial benefit of its shareholders or owners; 2. Does business in this state; 3. Collects personal information about consumers, or is the entity on behalf of which such information is collected; 4. Determines the purposes and means of processing personal information about consumers alone or jointly with others; and 5. Satisfies at least two of the following thresholds: (I) has global annual gross revenues in excess of $50 million, as adjusted in January of every odd-numbered year to reflect any increase in the Consumer Price Index. (II) Annually buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, or devices for targeted advertising in conjunction with third parties or that is not covered by an exception under this section. (III) Derives 50% or more of its global annual revenues from selling or sharing personal information about consumers. Controller also includes any entity that controls or is controlled by a controller. As used in this subparagraph, the term "control" means: 1. Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a controller; 2. Control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or 3. The power to exercise a controlling influence over the management of a company.
Definition of "***consumer***"	Consumer means a natural person who resides in or is domiciled in this state, however identified, including by any unique identifier, who is acting in a personal capacity or household context. The term does not include a natural person acting on behalf of a legal entity in a commercial or employment context.
Enforcement	· Attorney General & private right of action. · Damages are between $100 and $750 per consumer per incident. · Consumer can recover attorney fees. · AG *may* offer a 45-day cure period.

Maine[8]	
An Act to Protect the Privacy of Online Consumer Information [LD 946]	
Definition of "***customer***"	"Customer" means an applicant for or a current or former subscriber of broadband Internet access service.
Definition of "***provider***"	"Provider" means a person who provides broadband Internet access service.
Scope	Applies to providers on broadband internet access and prohibits them from using, disclosing, selling or permitting access to customer personal information except as provided in subsections 3 and 4, Title 16, chapter 3, subchapters 10 and 11 and 18 United States Code, Section 2703.

Exceptions	• Customer consent
	  ○ A. A provider may use, disclose, sell or permit access to a customer's customer personal information if the customer gives the provider express, affirmative consent to such use, disclosure, sale or access. A customer may revoke the customer's consent under this paragraph at any time.
	  ○ B. A provider may not: (1) Refuse to serve a customer who does not provide consent under paragraph A; or (2) Charge a customer a penalty or offer a customer a discount based on the customer's decision to provide or not provide consent under paragraph A.
	  ○ C. A provider may use, disclose, sell or permit access to information the provider collects pertaining to a customer that is not customer personal information, except upon written notice from the customer notifying the provider that the customer does not permit the provider to use, disclose, sell or permit access to that information.
	• Other exceptions. Notwithstanding the provisions of subsections 2 and 3, a provider may collect, retain, use, disclose, sell and permit access to customer personal information without customer approval:
	  ○ A. For the purpose of providing the service from which such information is derived or for the services necessary to the provision of such service;
	  ○ B. To advertise or market the provider's communications-related services to the customer;
	  ○ C. To comply with a lawful court order;
	  ○ D. To initiate, render, bill for and collect payment for broadband Internet access service;
	  ○ E. To protect users of the provider's or other providers' services from fraudulent, abusive or unlawful use of or subscription to such services; and
	  ○ F. To provide geolocation information concerning the customer:
	  ▪ (1) For the purpose of responding to a customer's call for emergency services, to a public safety answering point; a provider of emergency medical or emergency dispatch services; a public safety, fire service or law enforcement official; or a hospital emergency or trauma care facility; or
	  ▪ (2) To a provider of information or database management services solely for the purpose of assisting in the delivery of emergency services in response to an emergency

Enforcement	Public Utilities Commission (ME ST T. 35-A § 1508-A)
Notice requirement	A provider shall provide to each of the provider's customers a clear, conspicuous and non-deceptive notice at the point of sale and on the provider's publicly accessible website of the provider's obligations and a customer's rights under this section.

[8] This statute is more properly thought of as a public utilities law rather than a general consumer privacy statute.

Minnesota	
Minnesota Consumer Data Privacy Act [Ca. Civ. Code 1798.100, *et seq.*]	
Definition of "***consumer***"	"Consumer" means a natural person who is a Minnesota resident acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.
Definition of "***controller***"	"Controller" means the natural or legal person which, alone or jointly with others, determines the purposes of the processing of personal data.
Definition of "***personal data***"	"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. Personal data does not include deidentified data or publicly available information.
Definition of "***sensitive data***"	"Sensitive data" means: o personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sexual orientation, or citizenship or immigration status; o the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; o the personal data of a known child; or o specific geolocation data.
Scope	This Act applies to legal entities that conduct business in Minnesota or produce products or services that are targeted to residents of Minnesota, and that satisfy one or more of the following thresholds: o during a calendar year, controls or processes personal data of 100,000 consumers or more; or o derives over 25% of gross revenue from the sale of personal data; and o processes or controls personal data of 25,000 consumers of more.
Enforcement	Enforced by the Attorney General Any controller of processor that violates this chapter is subject to an injunction and liable for a civil penalty of more more than $7,500 for each violation.

Nevada	
Nevada Privacy of Information Collected On Internet From Consumers (NPICIC) [SB 220/Ch. 603A.300 – 603A.360]	
Definition of "***consumer***"	A person who seeks or acquires, by purchase or lease, any good, service, money or credit for personal, family or household purposes from the Internet website or online service of an operator.
Definition of "***covered information***"	Any one or more of the following personally identifiable information about a consumer collected by an operator through an Internet website or online service and maintained by the operator in an accessible form: 1. A first and last name. 2. A home or other physical address which includes the name of a street and the name of a city or town. 3. An electronic mail address. 4. A telephone number. 5. A social security number. 6. An identifier that allows a specific person to be contacted either physically or online. 7. Any other information concerning a person collected from the person through the Internet website or online service of the operator and maintained by the operator in combination with an identifier in a form that makes the information personally identifiable.
Definition of "***operator***"	A person who: a) Owns or operates an Internet website or online service for commercial purposes; b) Collects and maintains covered information from consumers who reside in this State an use or visit the Internet website or online service; and c) Purposefully directs its activities toward this State, consummates some transaction with this State or a resident thereof, purposefully avails itself of the privilege of conducting activities in this State or otherwise engages in any activity that constitutes sufficient nexus with this State to satisfy the requirements of the United States Constitution. [term exclusions listed in subsection 2]
Enforcement	Attorney General Penalty: (1) permanent injunction, or (2) civil penalty not to exceed $5,000 for each violation <u>*No*</u> private right of action.
Opt-Out	Consumer must submit a *verified request* Operator must respond within 60 days

New York	
Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) [S5575B] [NY Gen. Bus. Law §§ 899-aa; 899-bb]	
Definition of "***covered entity***"	The term "covered entity" is used in the SHIELD Act; however, no express definition is provided. The SHIELD Act also refers to "[a]ny person or business which owns or licenses computerized data which includes private information."
Definition of "***private information***"	Either: (i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired: 1. social security number; 2. driver's license number or non-driver identification card number; 3. account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account; 4. account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or 5. biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or (ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account. "Private information" does <u>not</u> include publicly available information which is lawfully made available to the general public from federal, state, or local government records.
Enforcement	Attorney General Penalty for violation of § 899-aa (notification of breach): (1) permanent injunction, (2) damages, and/or (3) civil penalty of the greater of $5,000 or up to $20/instance of failed notification (not to exceed $250,000) Penalty for violation of §§ 899-bb (data security protections): (1) permanent injunction and/or (2) civil penalty of not more than five thousand dollars for each violation <u>*No*</u> private right of action.
Proposed Legislation	New York Data Accountability and Transparency Act ("NYDATA") -- Governor Cuomo proposed a comprehensive data privacy law, which is quite similar to the CCPA and CPRA.

Oklahoma	
Oklahoma Computer Data Privacy Act (OCDPA) [HB1602]	
Definition of "***consumer***"	"Consumer" means an individual who is a resident of this state.
Definition of "***personal information***"	"Personal information" means information that identifies, relates to, describes, can be associated with or can reasonably be linked to, directly or indirectly, a particular consumer or household. The term includes the following categories of information if the information identifies, relates to, describes, can be associated with or can reasonably be linked to, directly or indirectly, a particular consumer or household: a. an identifier, including a real name, alias, mailing address, account name, date of birth, driver license number, unique identifier, Social Security number, passport number, signature, telephone number or other government-issued identification number, or other similar identifier, b. an online identifier, including an electronic mail address or Internet Protocol address, or other similar identifier, c. a physical characteristic or description, including a characteristic of a protected classification under state or federal law, d. commercial information, including: (1) a record of personal property, (2) a good or service purchased, obtained or considered, (3) an insurance policy number, or (4) other purchasing or consuming histories or tendencies, e. biometric information, f. Internet or other electronic network activity information, including: (1) browsing or search history, and (2) other information regarding a consumer's interaction with an Internet website, application or advertisement, g. geolocation data, h. audio, electronic, visual, thermal, olfactory or other similar information, i. professional or employment-related information, j. education information that is not publicly available personally identifiable information under the federal Family Educational Rights and Privacy Act of 1974, k. financial information, including a financial institution account number, credit or debit card number, or password or access code associated with a credit or debit card or bank account, l. medical information, m. health insurance information, or n. inferences drawn from any of the information listed under this paragraph to create a profile about a consumer that reflects the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities or aptitudes;
Scope	This act applies only to: 1. A business that: a. does business in this state, b. collects consumers' personal information or has that information collected on the business's behalf, c. alone or in conjunction with others, determines the purpose for and means of processing consumers' personal information, and d. satisfies one or more of the following thresholds: (1) has annual gross revenue in an amount that exceeds Ten Million Dollars ($10,000,000.00),

	(2) alone or in combination with others, annually buys, sells or receives or shares for commercial purposes the personal information of fifty thousand or more consumers, households or devices, or (3) derives twenty-five percent (25%) or more of the business's annual revenue from selling consumers' personal information; and 2. An entity that controls or is controlled by a business described by paragraph 1 of this subsection and that shares the same or substantially similar brand name and/or common database for consumers' personal information.
Exemptions	This act does not apply to: 1. Publicly available information; 2. Medical information governed by [HIPAA]; 3. A provider of health care, or a health plan, governed by [HIPAA], to the extent the provider or covered entity maintains, uses and discloses patient information in the same manner as medical information or protected health information as described in paragraph 2 of this subsection; 4. A business associate of a covered entity governed by [HIPAA], to the extent that the business associate maintains, uses and discloses patient information in the same manner as medical information or protected health information as described in paragraph 2 of this subsection; 5. Information that meets both of the following conditions: a. is de-identified in accordance with the requirements for de-identification set forth in Section 164.514 of Part 164 of Title 45 of the Code of Federal Regulations, and b. is derived from patient information that was originally collected, created, transmitted or maintained by…the Common Rule. 6. Information that is collected, used or disclosed in research… including, but not limited to, a clinical trial, and that is conducted in accordance with … the Common Rule; 7. The sale of personal information to or by a consumer reporting agency if the information is to be: a. reported in or used to generate a consumer report, as defined by Section 1681a(d) of the Fair Credit Reporting Act (15 U.S.C., Section 1681 et seq.), and b. used solely for a purpose authorized under that act; 8. Personal information collected, processed, sold or disclosed in accordance with: a. the federal Gramm-Leach-Bliley Act of 1999 (Public Law 106-102) and its implementing regulations, or b. the federal Driver's Privacy Protection Act of 1994 (18 U.S.C., Section 2721 et seq.); 9. De-identified or aggregate consumer information; or 10. A consumer's personal information collected or sold by a business, if every aspect of the collection or sale occurred wholly outside of this state. Provided further, nothing in this act shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder.
Enforcement	A person who violates this act is liable to this state for injunctive relief and/or a civil penalty in an amount not to exceed: 1. Two Thousand Five Hundred Dollars ($2,500.00) for each violation; or 2. Seven Thousand Five Hundred Dollars ($7,500.00) for each violation, if the violation is intentional. B. The Oklahoma Attorney General is entitled to recover reasonable expenses, including reasonable attorney fees, court costs and investigatory costs, incurred in obtaining injunctive relief or civil penalties, or both, under this section. Amounts collected under this section shall be deposited in a dedicated account in the General Revenue Fund and shall be appropriated only for the purposes of the administration and enforcement of this act.

Utah	
Utah Consumer Privacy Act [S.B. 200]	
Definition of "***Consumer***"	"Consumer" means an individual who is a resident of the state of Utah acting in an individual or household context.
Definition of "***Personal data***"	"Personal data" means any information that: o identifies or describes an identifiable individual; or o is reasonably capable of identifying or describing an identifiable individual. "Personal data" does not include deidentified data, anonymous or pseudonymous data, or publicly available information.
Definition of "**Sensitive data**"	"Sensitive data" means: o a personal data that reveals an individual's : o racial or ethnic origin; o religious beliefs; o diagnosed mental or physical health condition; o sexual orientation; o citizenship or immigration status; o the processing of genetic or biometric personal data for the purpose of identifying an individual; o the personal data of a known child; or o specific geolocation data.
Definition of "**Controlle**r"	"Controller" means a person doing business in the state who processes personal data solely for the purposes described in this Act.
Scope	This Act applies to any controller or processor who: o conducts business in Utah; or o produces a product or service that is targeted to residents of the state; and o satisfies one or more of the following thresholds: o during a calendar year, controls or processes personal data of 100,000 or more consumers; or o derives over 50% of the entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers.
Enforcement	Attorney General Penalty: Attorney General may recover actual damages to the consumer and for each violation of this Act, an amount not to exceed $1,000 per consumer affected by the violation. *No* private right of action.

Vermont	
Vermont's Security Breach Notice Act *[Bill S.110]*	
Definition of "***Consumer***"	"Consumer" means an individual residing in this State.
Definition of "***Personally identifiable information***"	"Personally identifiable information" means a consumer's first name or first initial and last name in combination with one or more of the following digital data elements, when the data elements are not encrypted, redacted, or protected by another method that renders them unreadable or unusable by unauthorized persons: (i) a Social Security number; (ii) a driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction; (iii) a financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords; (iv) a password, personal identification number, or other access code for a financial account; (v) unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data; (vi) genetic information; and (vii)(I) health records or records of a wellness program or similar program of health promotion or disease prevention; (II) a health care professional's medical diagnosis or treatment of the consumer; or (III) a health insurance policy number.
Definition of "***Business***"	"Business" means a commercial entity, including a sole proprietorship, partnership, corporation, association, limited liability company, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent, affiliate, or subsidiary of a financial institution, but does not include the State, a State agency, any political subdivision of the State, or a vendor acting solely on behalf of, and at the direction of, the State.
Definition of "***Data Collector***"	"Data collector" means a person who, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with personally identifiable information, and includes the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, and retail operators.
Enforcement	The Attorney General and State's Attorney shall have sole and full authority to investigate potential violations of this subchapter and to enforce, prosecute, obtain, and impose remedies for a violation of this subchapter or any rules or regulations made pursuant to this chapter as the Attorney General and State's Attorney have under chapter 63 of this title. The Attorney General may refer the matter to the State's Attorney in an appropriate case. The Superior Courts shall have jurisdiction over any enforcement matter brought by the Attorney General or a State's Attorney under this subsection. With respect to a data collector that is a person or entity licensed or registered with the Department of Financial Regulation under Title 8 or this title, the Department of Financial Regulation shall have the full authority to investigate potential violations of this subchapter and to prosecute, obtain, and impose remedies for a violation of this subchapter or any rules or regulations adopted pursuant to this subchapter, as the Department has under Title 8 or this title or any other applicable law or regulation. • A person who violates a provision of this chapter commits an unfair and deceptive act in commerce. • No private right of action.

Virginia	
Consumer Data Protection Act [SB 1392 Consumer Data Protection Act; personal data rights of consumer, etc.]	
Definition of "***consumer***"	"Consumer" means a natural person who is a resident of the Commonwealth acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.
Definition of "***controller***"	"Controller" means the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data.
Scope	A. This chapter applies to persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that (i) during a calendar year, control or process personal data of at least 100,000 consumers or (ii) control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data.
Exemptions	• Does not apply to the following entities (total exemption): (i) body, authority, board, bureau, commission, district, or agency of the Commonwealth or of any political subdivision of the Commonwealth; (ii) financial institution or data subject to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.); (iii) covered entity or business associate governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164 established pursuant to HIPAA, and the Health Information Technology for Economic and Clinical Health Act (P.L. 111-5); (iv) nonprofit organization; or (v) institution of higher education. • There are 14 data-specific exemptions, *e.g.*, Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (12 U.S.C. § 2001 et seq.); Personal data regulated by the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g et seq.). • Controllers and processors that comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) shall be deemed compliant with any obligation to obtain parental consent under this chapter
Enforcement	§ 59.1-580. Enforcement; civil penalty; expenses. A. The Attorney General shall have exclusive authority to enforce the provisions of this chapter. B. Prior to initiating any action under this chapter, the Attorney General shall provide a controller or processor 30 days' written notice identifying the specific provisions of this chapter the Attorney General alleges have been or are being violated. If within the 30-day period, the controller or processor cures the noticed violation and provides the Attorney General an express written statement that the alleged violations have been cured and that no further violations shall occur, no action shall be initiated against the controller or processor. C. If a controller or processor continues to violate this chapter following the cure period in subsection B or breaches an express written statement provided to the Attorney General under that subsection, the Attorney General may initiate an action in the name of the Commonwealth and may seek an injunction to restrain any violations of this chapter and civil penalties of up to $7,500 for each violation under this chapter. D. The Attorney General may recover reasonable expenses incurred in investigating and preparing the case, including attorney fees, in any action initiated under this chapter. E. Nothing in this chapter shall be construed as providing the basis for, or be subject to, a private right of action for violations of this chapter or under any other law.
Opt-Out and Appeals	Consumer must submit an authenticated request ("Authenticate" means verifying through reasonable means that the consumer, entitled to exercise his consumer rights in § 59.1-573, is the same consumer exercising such consumer rights with respect to the personal data at issue) Controller must respond within 45 days, although an additional 45 days is permissible if necessary and the controller informs the consumer of the extension within the initial 45 day response period. A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision pursuant to subdivision B 2. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to subsection A. Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the

	reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

Washington	
Washington Privacy Act [SSB 5062]	
Definition of "***consumer***"	A natural person who is a Washington resident acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.
Definition of "***covered information***"	"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include deidentified data or publicly available information.
Definition of "***covered entity*** "	Legal entities that conduct business in Washington or produce products or services that are targeted to residents of Washington, and that satisfy one or more of the following thresholds: a) During a calendar year, controls or processes personal data of one 100,000 consumers or more; or b) Derives over fifty percent of gross revenue from the sale of personal data **and** processes or controls personal data of 25,000 consumers or more.
Definition of "**controlle**r"	The natural or legal person that, alone or jointly with others, determines the purposes and means of the processing of personal data.
Enforcement	Attorney General Penalty: Cap for civil penalties for controllers and processors in violation of the Act at $7,500 per violation. The current version of the bill includes a 30 day right to cure alleged violations. *No* private right of action.
Opt-Out	A consumer has the right to opt out of the processing of personal data concerning such a consumer for the purposes of: (a) targeted advertising; (b) the sale of personal data; or (c) profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer. Consumer can submit a specific request at any time to controller of data. Controller must comply with request no later than 15 days from the receipt of the request.