State Data Privacy Law Tracker

A concise update on the status and content of state consumer data privacy protection laws — both proposed and enacted — compiled by the attorneys of Fox Rothschild's Privacy & Data Security Practice Group.

Fox Rothschild LLP
ATTORNEYS AT LAW

Table of Contents

Compiled by Fox Rothschild Associates:
Ciera Logan, Atlantic City; **Kristina Neff Burland**, Philadelphia; and **Alanna Elinoff**, Chicago.

Following California's Lead: State Consumer Data Privacy Protection Laws

Enacted in 2018, the California Consumer Privacy Act (CCPA) is scheduled to take effect in 2020, posing a host of new data privacy compliance challenges for companies with customers in California or clients who do business in the state, which is the sixth-largest economy in the world.

The new law — which has quickly become a model for others states' privacy legislation — affects for-profit companies that collect and process California residents' personal information, have business in the state and meet one of the following three criteria:

- Generate annual gross revenue > $25 million
- Receive or share data of > 50,000 California residents annually
- Derive at least 50 percent of annual revenue by selling California residents' personal information

Companies that fall under the act must also ensure that any service providers that handle data on their behalf do it in a manner that complies with the law.

CCPA includes a broad definition of personal information and conveys new rights designed to give consumers more control over their data. These include the ability to opt out of having their data sold, to request information on the types of data companies collect and/or a copy of the actual data collected and, in many cases, the right to request that their data be erased.

The law includes per capita fines of up to $2,500 per incident for violations and up to $7,500 per incident for willful violations, and includes a limited private right of action that allows consumers to file lawsuits over data breaches under certain circumstances.

In the aftermath of the passage of CCPA, a growing number of other states have proposed, and in some cases adopted, similar new laws. However, each is unique and contains provisions that depart from the CCPA in important ways. In addition, California has amended its original legislation.

This handy guide summarizes key components of state data privacy laws that have been proposed and enacted across the United States, presenting the information in an easy-to-read chart format, as well as providing an update on the status of pending legislation as of **Oct. 9, 2019.**

Fox Rothschild Privacy & Data Security

Data Privacy Compliance

HIPAA, GDPR, CCPA. Data privacy compliance has become an alphabet soup of federal, state and international acronyms. Fox Rothschild has the knowledge and experience to help clients avoid costly fines and comply with the myriad regulations that govern the data they collect. We help companies comply with state privacy, data security and data reporting laws as well as international privacy and security requirements.

HIPAA Compliance

Fox understands that compliance with the Health Insurance Portability and Accountability Act (HIPAA) isn't limited to hospitals and medical practices. We provide comprehensive services focused on the proper handling of Protected Health Information (PHI) that include:

- Preparing required policies and procedures for health care providers, health plans and business associates
- Drafting business associate agreements, data use agreements for health information exchanges accessed by multiple providers, HIPAA-compliant authorizations for disclosure of PHI and access request forms to be used by covered entities for patient or plan member PHI access requests
- Providing HIPAA compliance reviews for researchers receiving or using PHI
- Reviewing mergers/acquisitions of HIPAA-covered entities and business associates: due diligence and handling PHI; representations and warranties related to HIPAA compliance and breaches discovered after closing
- Providing breach and security incident response and analysis.
- Responding to Office of Civil Rights (OCR) investigations.

GDPR Compliance

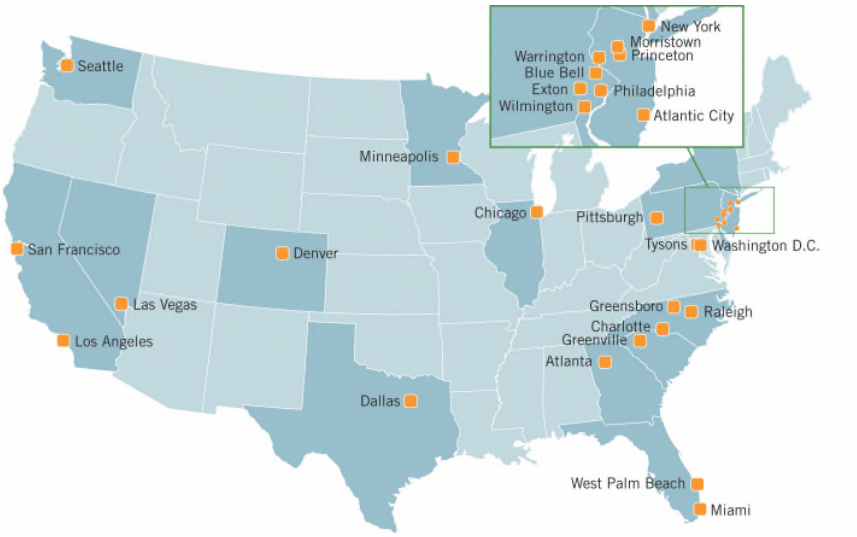
Our team works with clients to assess their exposure to the European Union's General Data Protection Regulation (GDPR) and design policies and procedures to mitigate risks. We use our detailed knowledge of EU data protection law, coupled with our understanding of the unique challenges it poses to U.S.-based corporations, to create pragmatic, actionable, tailored plans to achieve GDPR compliance.

CCPA Compliance

We help companies prepare for The California Consumer Privacy Act (CCPA). Scheduled to take effect in 2020, the CCPA will change the way companies both inside and outside the state manage consumers' personal data by conferring a new set of rights on consumers and a new set of responsibilities on the companies that handle their data. We help clients determine their exposure, catalog the data they collect and how it is used, and update their privacy policies, procedures and websites to bring them into compliance with this new law.

The Fox Difference

Fox Rothschild is a leader. We've been named to the Law Firms Best at Cybersecurity Honor Roll by BTI, a respected provider of client-based data for the legal industry. When you choose Fox, you get Privacy & Data Security attorneys who are nationally recognized:



- Team members who are CIPP/US, CIPP/E, and CIPM certified by the International Association of Privacy Professionals and CDPO certified by the Professional Evaluation and Certification Board.
- Partners named Trailblazers in Cybersecurity Law by the *National Law Journal*.
- Chambers-ranked attorneys.

Our lawyers are frequent speakers on safeguarding sensitive information and new developments in privacy. The team includes attorneys who are frequently quoted on issues of privacy and data security by national media outlets such as *The Economist, The Wall Street Journal, The New York Times, Forbes, The Huffington Post and Compliance Week.*

We're also one of few firms in the country that has its own Chief Privacy Officer and HIPAA Privacy & Security Officer.

Part of a law firm with 950 attorneys in offices coast-to-coast, Fox Rothschild's Privacy & Data Security team delivers the service and focus of a boutique with the reach and resources of a national law firm.

Key Contacts

ODIA KAGAN
Partner and Chair of GDPR Compliance and International Privacy
okagan@foxrothschild.com

ELIZABETH LITTEN
Partner and HIPAA Privacy & Security Officer | Co-chair, Privacy & Data Security Practice
elitten@foxrothschild.com

MARK G. MCCREARY
Partner and Chief Privacy Officer | Co-chair, Privacy & Data Security Practice
mmccreary@foxrothschild.com

State Consumer Data Privacy Protection Laws Snapshot

Following California's adoption of the California Consumer Privacy Act (CCPA) in 2018, lawmakers in multiple states have proposed, and in some cases enacted, similar laws aimed at safeguarding consumer data.

The following table provides a summary of the status, and key provisions in those laws as of DATE.

LEGISLATIVE HISTORY

State	Status	Effective Date (if applicable)	Link to Text
California	Passed	1/1/2020	AB 375
Connecticut	Passed	7/9/2019	CT SB 1108
Nevada	Passed	10/1/2019	SB 220
Hawaii	Bill		SB 418
Illinois	Bill		HB 3358
Louisiana	Adopted		HR 249
Maine	Enacted	7/1/2020	ME SB 275
Maryland	Bill		SB 613
Massachusetts	Bill		SD 341
Minnesota	Regular session adjourned; carryover pending		"MN HF 1030 (Same as SF 433)"
Minnesota	Regular session adjourned; carryover pending		"MN HF 2917 (Same as SF 2912)"
Mississippi	Bill		HB 1253
New Jersey	Bill		AB 4640
New Mexico	Bill		SB 176
New York	Bill		SB 224
Pennsylvania	Bill		HB 1049
Washington	Bill		SB5376

BUSINESSES COVERED

State	Minimum revenue to meet definition of covered business	# of consumers to meet definition of covered business	% annual revenue to meet definition of covered business
California	$25 million	50,000+	50 percent
Connecticut	No	No	No
Nevada	No, per Nevada's previously passed law 603A	No, per Nevada's previously passed law 603A	No, per Nevada's previously passed law 603A
Hawaii	No	No	No
Illinois	None	>50,000	50 percent or more
Louisiana	No	No	No
Maine	No	No	No
Maryland	No	100,000+	50 percent
Massachusetts	No	None.	50 percent
Minnesota	No	No	No
Minnesota	No	100,000	50 percent of gross revenue from sale of personal information (AND process or control personal information of at least 25,000 consumers)
Mississippi		50,000+	50 percent
New Jersey	No	No	50 percent
New Mexico	No	No	No
New York	No	No	No
Pennsylvania	$10 million	50,000	50 percent
Washington	None	100,000	50 percent of gross revenue AND processes or controls personal data of at least 25,000 consumers.

CONSUMER PROTECTIONS

State	Access to Personal Info Collected	Access to Personal Information Shared	Right to Correction	Right to Deletion	Right to Data Portability
California	Yes	Yes	No	Yes	Yes
Connecticut	No	No	No	No	No
Nevada	Yes, per Nevada's previously passed law 603A	No	No	No	No
Hawaii	Yes	Yes	No	Yes	No
Illinois	No	Yes	No	No	No
Louisiana	No	No	No	No	No
Maine	No	No	No	No	No
Maryland	Yes	No	No	Yes	Yes
Massachusetts	Yes	Yes	No	Yes	Yes
Minnesota (HF 1030)	No	No	No	No	No
Minnesota (HF 2917)	Yes	Yes	Yes	Yes	Yes
Mississippi	Yes	Yes	No	Yes	Yes
New Jersey	Yes	Yes	Yes	No	Yes
New Mexico	Yes	Yes	No	Yes	Yes
New York	Yes	Yes	No	No	No
Pennsylvania	Yes	Yes	No	Yes	No
Washington	Yes	Yes	Yes	Yes	Yes

CONSUMER RIGHTS & ENFORCEMENT

State	Opt Out	Children	Private right of action	Vendor Provisions
California	Yes	Yes	Yes	Yes
Connecticut	Yes	No	No	No
Nevada	Yes	No	None	No
Hawaii	Yes	Yes	None	No
Illinois	Yes	No	No	No
Louisiana	No	No	No	No
Maine	Yes (referred to as Opt In)	No	No	No
Maryland	Yes	Yes	No	Yes
Massachusetts	Yes	Yes	Yes	Yes
Minnesota	Yes	No	No	Yes
Mississippi	Yes	Yes	Yes	Yes
New Jersey	Yes	No	Yes	Yes
New Mexico	Yes	Yes	Yes	Yes
New York	Yes	No	Yes	Yes
Pennsylvania	Yes	Yes	Yes	No
Washington	No	No	No	Yes

Detailed State-by-State Analysis

California

California Consumer Privacy Act, AB 375

- Legislative Status: Passed
- Effective Date: 1/1/2020
- Link to Text: AB 375

California's Consumer Rights Checklist	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** is defined as a natural person who is a California resident

- ***Personal Information*** is defined as information that identifies, relates to, describes, is associated with, or could reasonably be linked, directly or indirectly with a customer, and includes:

  - 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

  - Personal information like address, signature, social security number, telephone number, any identification numbers, any banking identification numbers, and employment history

- Protected classifications under California or federal law
- Commercial information, like personal property records, products or services purchased or considered, or other purchasing or consuming histories or tendencies
- Biometric information
- Internet or other electronic network activity information, including browsing history and information regarding a consumer's interaction with an Internet Web site, application, or advertisement
- Geolocation data
- Audio, electronic, visual, or similar information
- Professional or employment-related information
- Education information
- Inferences drawn about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, and intelligence

**Personal information does not include publicly available information.*

- ***Business*** is defined as a for profit legal entity that does business in the State of California and collects consumers' personal information, or on the behalf of which such information is collected, determines the purposes and means of processing consumers' personal information. The business must satisfy one or more of the following thresholds:
  - Has annual gross revenues in excess of $25 million ($25,000,000).
  - Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices.

- Derives 50 percent or more of its annual revenues from selling consumers' personal information.

❖ ***Business*** is also defined as an entity that controls or is controlled by a business, as defined above, and shares common branding with the business

Enforcement

❖ ***Enforcement***

- The attorney general may bring a civil action to recover penalties

❖ ***Private Right of Action***

- A consumer may bring a civil action for any of the following:
  - To recover damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater; or
  - Injunctive or declaratory relief.

Data Safe Harbors

❖ Personal information collected by a covered entity governed by the Confidentiality of Medical Information Act or governed by the privacy, security, and breach Notification rules established under HIPAA

❖ Sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report

❖ Personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (GLBA)

❖ Personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994

❖ To comply with federal, state, or local laws

- Comply with civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities
- Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law
- Exercise or defend legal claims
- Collect, use, retain, sell, or disclose consumer information that is de-identified or in the aggregate consumer information
- Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside California

Vendor Provisions

- The CCPA prohibits a third party from selling personal information about a consumer that was sold to the third party by a business, unless the consumer received explicit notice and is provided an opportunity to exercise the right to opt out

Hawaii

Relating to Privacy

- Legislative Status: Referred to CPS, JDC 1/24/2019
- Link to Text: SB 418

Hawaii's Consumer Rights Checklist	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction	✓	

Key Definitions

- ***Consumer*** means an individual who interacts with a business within the state

- ***Identifying Information*** means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked with a particular consumer or household, including:

  - Name, alias, postal address, unique identifier, Internet Protocol address, email address, account name, social security number, driver's license number, or passport number, signature, Biometric information;

  - Protected classifications;

  - Commercial information, including records of personal property, products, or services purchased, obtained, or considered, or other purchasing or consuming history or tendencies;

  - Biometric information

- Internet and other electronic network activity information including browsing history, search history, and information regarding a consumer's interaction with an internet web site, application, or advertisement;
- Geolocation data;
- Audio, electronic, visual, or similar recordings Professional or employment-related information;
- Education records;
- Medical data;
- Insurance information;
- Financial information; or
- Profiles about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, or intelligence created from inferences from any other information collected from a consumer.

❖ Hawaii's law does Not define ***Business***

Enforcement

❖ ***Enforcement***

- This law shall be enforced by the office consumer protection

❖ There is No ***Private Right of Action***

There are no ***Data Safe Harbors***

There are no ***Vendor Provisions***

Illinois

Data Transparency and Privacy Act

- Legislative Status: Re-referred to Assignments; 5/31/2019
- Link to Text: HB3358

Consumer Rights	Yes	No
Access to Personal Information Collected		✓
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion		✓
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out	✓	
Children		✓
Data Destruction		✓

Key Definitions

- ***Consumer*** is defined as a resident of Illinois who provides personal information to a private entity, in the course of purchasing, viewing, accessing, renting, leasing, or otherwise using real or personal property, or any interest therein, or obtaining a product or service from the private entity, including advertising or any other content.

  Consumer does not include a person from whom personal information is collected while that person is acting in an employment context.

- ***Personal Information*** is defined as any information that is linked or can reasonably be linked, to a particular consumer, including name, alias, signature, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, bank account number, credit card number, debit card number, or any other financial account information, unique personal identifier, geolocation, or biometric information.

- ***Business*** is defined as a for profit legal entity that does business in the State of Illinois, and satisfies one or more of the following thresholds:

- Has annual gross revenues in excess of $25 million ($25,000,000).
- 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; or
- Derives 50 percent or more of its annual revenues from selling consumers' personal information.

Enforcement

- ***Enforcement***
  - The Attorney General has exclusive authority to enforce this Act
- There is no ***Private Right of Action***

Data Safe Harbors

- Disclosure of personal information by a private entity under a written contract authorizing the third party to utilize the personal information for limited purposes of performing services on behalf of the private entity
- Disclosure of personal information based on a good faith belief that disclosure is required to comply with applicable law, regulation, legal process, or court order; or
- Disclosure of personal information by a private entity to address fraud, security, or technical issues, to protect the disclosing private entity's rights or property, or to protect consumers or public from illegal activities;
- Health care provider or other covered entity subject to HIPAA;
- Financial institution or subject to GLBA; and
- To a contractor, subcontractor, or agent of a state agency or local unit of government when working for that state agency or local unit of government;
- See full list at link provided above

Vendor Provisions

- If a third party materially alters how it uses or shares personal information in a manner that is inconsistent with the promises made at the time of collection, it shall provide prior notice of the changed practice to the consumer.

Maine

Broadband Internet Access Service Customer Privacy

- Legislative Status: Enacted
- Effective Date: 7/1/2020
- Link to Text: ME SB 275 (LD 946)

Maine Consumer Rights Checklist	Yes	No
Access to Personal Information Collected		✓
Access to Personal Information Shared		✓
Right to Correction		✓
Right to Deletion		✓
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt In	✓	
Children		✓
Data Destruction		✓

Key Definitions

- ***Customer*** is defined as applicant for or a current or former subscriber of broadband Internet access service

- ***Personal Information*** is defined as personally identifying information about a customer, including name, billing information, Social Security number, billing address and demographic data; and information form a customer's use of broadband internet access service including web browsing history, usage history, precise geolocation information, financial information, health information, information pertaining to the customer's children, the origin and destination internet protocol address, or the content of the customer's communications the customer's device identifier, such as a media access control address, international mobile equipment identity or Internet protocol address.

- ***Provider*** is defined as a person or provider who provides broadband internet access service within the state to customers physically located and billed for service received in the state.

Enforcement

- There is no ***Enforcement*** provision

- There is no ***Private Right of Action***

Data Safe Harbors

- Information obtained for the purpose of providing the service from which such information is derived or for the services necessary to the provision of such service;
- To advertise or market the provider's communications-related services to the customer;
- To comply with a lawful court order;
- To initiate, render, bill for and collect payment for broadband internet access service;
- To protect users of the provider's or other providers' services from fraudulent, abusive or unlawful use of or subscription to such services; and
- To provide geolocation information concerning the customer to respond to emergency services

There are no ***Vendor Provisions***

Maryland

Online Consumer Protection Act

- Legislative Status: In the Senate
- Effective Date:
- Link to Text: SB 613

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion		✓
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** means any individual who resides in Maryland.

- ***Personal Information*** means any information relating to an identified or identifiable consumer and information that identifies relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or the consumer's device.

  Personal Information does not include:

  - Information that is lawfully made available from federal, state, or local government records; or

  - Consumer information that is de-identified or aggregate consumer information.

- ***Business*** means any for-profit legal entity that collects the personal information of state consumers; and satisfies one or more of the following thresholds:

- Has annual gross revenues in excess of $25 million ($25,000,000);
- Annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 100,000 or more consumers, households, or devices; or
- Derives at least half of its annual revenues from selling consumers' personal information.

- A ***Business*** may also be defined as an entity that controls or is controlled by a business as defined above and shares a name, service mark, or trademark with the business.

Enforcement

- ***Enforcement***
  - When the Office of the Attorney General has a reason to believe that the act has been violated, the Attorney General may bring an action to restrain the violation by temporary restraining order or preliminary or permanent injunction and seek a civil penalty not exceeding $2,500 for each violation or not exceeding $7,500 for each intentional violation.
- There is no ***Private Right of Action***

Data Safe Harbors

- A business collecting or disclosing personal information of the business's employees if the business is collecting or disclosing the information within the scope of its role as an employer.
- Health information collected by a Covered Entity or Business Associate.
- A Covered Entity governed by the Privacy, Security, and Breach Notification Rules established in accordance with HIPAA.
- Information collected as part of a clinical trial subject to the Federal Policy For The Protection Of Human Subjects.

- Sale of personal information to or from a consumer reporting agency if that information is to be used to generate a consumer report.
- Personal information processed under the GLBA.
- Personal information processed under the Federal Driver's Privacy Protection Act Of 1994.
- Education information covered by the Federal Family Educational Rights And Privacy Act.

There are no ***Vendor Provisions***

Massachusetts

An Act Relative to Consumer Data Privacy

- Legislative Status: In the House; 1/22/19
- Link to Text: SD 341

Massachusetts Consumer Rights Checklist	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** means a natural person who resides in Massachusetts

- ***Personal Information*** means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or the consumer's device.

  Personal Information does not include consumer information that is identified or aggregate consumer information.

- ***Business*** means a for-profit legal entity that collects Massachusetts consumers' personal information; and satisfies one or more of the following thresholds:

  - Has annual gross revenues in excess of $10 million ($10,000,000) or

  - Derives 50 percent or more of its annual revenues from third party disclosure of consumers' personal information.

- A ***Business*** also refers to any entity that controls or is controlled by a business, as defined above, and shares common branding with the business.

Enforcement

- ***Enforcement***
  - The Attorney General may bring an action for a temporary restraining order or an injunction. In addition, the Attorney General may seek a civil penalty of not more than $2,500 for each violation or $7,500 for each intentional violation.
- ***Private Right of Action***
  - A consumer may bring a civil action for any of the following:
    - Damages in the amount not greater than $750 per incident or actual damages;
    - Injunctive or declaratory relief;
    - Reasonable attorney fees and costs; and
    - Any other relief the court deems proper.

Data Safe Harbors

- A business collecting or disclosing personal information of the business's employees so long as information is within scope of its role as employer.
- Health information collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services in 45 C.F.R. parts 160 and 164
- A covered entity governed by the privacy, security, and breach notification rules under the HIPAA

- Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects
- Sale of personal information to or from a consumer reporting agency if information is to be used to generate a consumer report under the Fair Credit Reporting Act
- Personal information collected, processed, sold, or disclosed under the GLBA
- Personal information collected, processed, sold, or disclosed under the Driver's Privacy Protection Act
- Education information covered by the Federal Family Educational Rights and Privacy Act

There are no ***Vendor Provisions***

Minnesota

Consumer Rights to Personal Data Processing

- Date Introduced: 5/19/2019
- Link to Text: MN HF 2917

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children		✓
Data Destruction		✓

Key Definitions

- ***Consumer*** means a resident of Minnesota. A consumer does not include a business's employee or contractor acting in the role of an employee or contractor.

- ***Personal Data*** means any information relating to an identified or identifiable person. Personal data does not include de-identified data.

- ***Controller*** means the natural or legal person that alone or jointly determines the purposes and means to process personal data. Controller also means legal entities that conduct business in Minnesota or produce products or services intentionally targeted to Minnesota residents, provided the entity:

  - controls or processes data of 100,000 consumers or more; or

  - derives over 50 percent of gross revenue from the sale of personal information, and

  - processes or controls the personal information of 25,000 consumers or more.

Enforcement

- ***Enforcement***
  - The attorney general may seek up to $2,500 for each violation and up to $7,500 for each intentional violation

- There is no ***Private Right of Action***

Data Safe Harbors

- This Act does not provide to government entities

- This Act does not apply to information collected pursuant to HIPAA, HITECH, GLBA,

- This Act does not apply to information collected solely for employment record purposes

Vendor Provisions

- Processing by a processor must be governed by a contract between the controller

Mississippi

The Mississippi Consumer Privacy Act of 2019

- Legislative Status: Died in Committee
- Link to Text: HB 1253

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** means a natural person who is a Mississippi resident.

- ***Personal Information*** means information that identifies, relates to, describes, is capable of being associated with, directly or indirectly, with a consumer or household. Personal information includes:

  - Identifiers such as real name, postal address, online identifier internet protocol address, email address, account name SSN, driver's license number, passport number

  - Characteristics of protected classifications under Mississippi or federal law;

  - Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;

  - Biometric information;

- Internet or other electronic network activity information,;
- Geolocation data;
- Audio, electronic, visual, thermal, olfactory or similar information;
- Professional or employment-related information; and
- Education information, defined as information that is not publicly available personally identifiable information; and
- Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer
- Personal information does not include publically available information.

❖ ***Business*** means a for-profit corporation, association, or other legal entity that collects consumers' personal information, or on the behalf of which such information is collected and determines the purposes and means of the processing of consumers' personal information, does business in the State of Mississippi, and satisfies one or more of the following thresholds:

- Has annual gross revenues in excess of $25 million ($25,000,000);
- Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, personal information of $50,000 or more consumers, households, or devices; or
- Derives 50 percent or more of its annual revenues from selling consumers' personal information; and
- A ***Business*** is also defined as any entity that controls or is controlled by a business, as defined above, and shares common branding with the business. "

Enforcement

❖ ***Enforcement***

- The Attorney General is authorized to enforce the act

- There is a ***Private Right of Action***

Data Safe Harbors

- This Act does not apply to:
  - Information subject to Fair Credit Reporting Act, HIPAA, GLBA, Driver's Privacy Protection Act

Vendor Provisions

- A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out

Nevada

Relating to Internet Privacy

- Legislative Status: Enrolled
- Effective Date: 10/1/2019
- Link to Text: SB 220, 603A

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared		✓
Right to Correction		✓
Right to Deletion		✓
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out	✓	
Children		✓
Data Destruction	✓	

Key Definitions

- ***Consumer*** means 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

- ***Personal Information*** means a natural person's first name or first initial and last name in combination with any of the following:

  - Social Security number, driver's license number, driver authorization card number or identification card number;

  - 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 the person's financial account;

  - A medical identification number or a health insurance identification number

- A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account.

❖ ***Operator*** means a person who

- owns or operates an internet website or online service for commercial purposes;
- Collects and maintains covered information from consumers who reside in this state and use or visit the internet website or online service; and
- Purposefully directs its activities toward this state, consummates some transaction with this state or a resident thereof or purposefully avails itself of the privilege of conducting activities in this state or otherwise engages in any activity that constitutes sufficient nexus with Nevada

Enforcement

❖ ***Enforcement***

- The Attorney General may
  - Issue an injunction or
  - Impose a civil penalty not to exceed $5,000 for each violation

❖ There is no ***Private Right of Action***

Data Safe Harbors

❖ This Act does not apply to

- Third parties who operate, host or manage a website on behalf of its owner or process information on behalf of the owner of an internet website
- Financial institutions or an affiliate of a financial institution subject to the GLBA
- Entities subject to the HIPAA

- A manufacturer of a motor vehicle or person who services a motor vehicle

Vendor Provisions

- A contract for the disclosure of personal information of a Nevada resident maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.

New Jersey

Assembly Bill 4640

- Legislative Status: Transferred to Assembly Homeland Security and State Preparedness Committee; 10/22/2018
- Link to Text: AB 4640

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion		✓
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children		✓
Data Destruction		✓

Key Definitions

- ***Data subject*** means an individual within New Jersey who provides, either knowingly or unknowingly, personally identifiable information to a business.

- ***Personal Identifiable Information*** means any information that personally identifies, describes, or is able to be associated with a data subject, including but not limited to:

  - Name, alias, nickname, and user name;
  - Postal and electronic mail address;
  - Telephone number;
  - Account name;
  - Social Security number or other government-issued identification number, birthdate or age;

- Physical characteristic information, including height and weight;
- Biometric data
- Sexual information (including sexual orientation, sex, gender status)
- Race or ethnicity;
- Religious affiliation or activity,
- Political affiliation or activity;
- Professional or employment-related information;
- Educational information
- Medical information;
- Financial information;
- Commercial information (including records of property, products, or services provided, obtained or considered, or other purchasing or consumer histories);
- Geolocation information;
- Internet or mobile activity information, including IP addresses or information concerning the access or use of any online service;
- Content, including text, photographs, audio or video recordings, or other material generated by or provided by the data subject; and
- Any of the above categories of information concerning children of the data subject.

- ***Business*** means a corporation, partnership, firm, enterprise, franchise, association, trust, sole proprietorship, union, political organization, or other legal entity other than a state agency (or any subdivision or contractor thereof) or federal agency that does business in New Jersey and has:
  - An annual gross revenue of $5 million ($5,000,000) or more;
  - Derives 50 percent or more of its annual revenue from selling the personally identifiable information of data subjects; or
  - Alone or in combination, annually buys, receives, sells, or shares for commercial purposes the personally identifiable information of at least 25,000 data subjects.

Enforcement

- ***Enforcement***
  - ***Private Right of Action***
    - A consumer may bring a civil action of not less than $100 and not more than $750 per security incident

Data Safe Harbors

- The requirements imposed shall not restrict a business's ability to:
  - Comply with federal, state, or local law;
  - Comply with a civil, criminal, or regulatory inquiry, investigation, or summons by federal, state, or local authorities;
  - Cooperate with law enforcement agencies or exercise or defend legal claims; or
  - Collect, use, retain, sell, or disclose a data subject's personally identifiable information that has been dei-dentified or in aggregate data subject information.

Vendor Provisions

- Although a business must allow a data subject to opt out of processing its personally identifiable information (PI"), this requirement does not apply where the processing of a data subject's PII occurs pursuant to a written contract between a business and third party, and where that contract prohibits the third party from using the PII for any reason other than performing the specified service and from disclosing PII to additional third parties

New Mexico

Consumer Information Privacy Act

- Legislative Status: action postponed indefinitely in Senate.
- Effective Date:
- Link to Text: SB0176

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** is not specifically defined by the statute.
  - However, Section 7 of the act sets forth certain limitations in scope, which are relevant to how the definition of consumer is construed. The act does not apply to the collection or sale of personal information if "every aspect of the business's commercial conduct occurs wholly outside the state. Commercial conduct takes place wholly outside of the state if the business collected that information while the consumer was outside of the state, no part of the sale of the consumer's personal information occurred in the state and no personal information collected while the consumer was in the state is sold.

- ***Personal Information*** is defined as information from federal, state, or local government records that identifies, describes or could reasonably be linked with a particular consumer or household, including:
  - A real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, bank account number, credit card number, debit card number, driver's license or state identification card number, insurance policy number, Social Security number, passport number or telephone number;

- Any information that identifies or is capable of being associated with a particular individual, including a signature, physical characteristic or description, education, employment, employment history, financial information, medical information, or health insurance information;
- Characteristics of protected classifications under state or federal law;
- Commercial information, including records of personal property, purchases of products or services or histories of purchases;
- Biometric information;
- Internet or other electronic network activity information;
- Geolocation data;
- Audio, electronic, visual, thermal, olfactory or similar information;
- Inferences drawn from any of the information identified above to create a profile about a consumer that reflects the consumer's preferences, characteristics, psychological trends, behaviors; or

Personal Information does not include publicly available information.

- ***Business*** means a corporation, joint venture, limited liability company, partnership, limited partnership, limited liability partnership, real estate investment trust or sole proprietor; or an entity that is controlled by any such entity.

Enforcement

- ***Enforcement***
  - The Office of the Attorney General may bring civil enforcement actions for violations.

- ***Private Right of Action.***
  - Any consumer whose non-encrypted or non-redacted personal information is subject to an unauthorized access and exfiltration, theft or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect

the personal information may file a civil action to recover actual damages; for injunctive relief; for statutory damages up to $750 per single occurrence or any other relief deemed proper by the court. Any action for statutory damages must comply with certain procedural requirements.

Data Safe Harbors

- To comply with federal, state or local laws;
- To comply with civil, criminal, or regulatory inquiry, an investigation, a subpoena or a summons by federal, state or local authorities;
- To cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state or local law;
- To exercise or defend legal claims;
- To collect, use, retain, sell or disclose consumer information that is de-identified or is in aggregate consumer information; or
- To collect or sell a consumer's personal information if every aspect of the business' commercial conduct takes place wholly outside of the state

Vendor Provisions

- The New Mexico bill prohibits a third party from selling personal information about a consumer that was sold to the third party by a business, unless the consumer received explicit notice and is provided an opportunity to exercise the right to opt out of the sale.
- Upon receipt of a request to delete the consumer's personal information from its records, the business must notify any service providers to delete the consumer's personal information from their records.

New York

Right to Know Act

- Legislative Status: Failed
- Link to Text: SB 224

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion		✓
Right to Data Portability		✓
Privacy Notice Required		✓
Opt Out		✓
Children		✓
Data Destruction		✓

Key Definitions

- ***Customer*** is defined as a New York resident who provides personal information to a business. An individual is also a customer of a business if that business obtained the individual's personal information from any other business.

- ***Personal Information*** is defined as any information that identifies or references a particular individual or electronic device or any information that relates to or describes an individual if disclosed in connection with identifying/referencing information. The definition includes name, alias, address, phone number, email, IP address, account name, SSN, driver's license number, passport number and any other identifier intended to be uniquely associated with a particular individual or device.

- ***Business*** is defined as any person, proprietorship, firm, partnership, cooperative, nonprofit organization or corporation organized or existing under the laws of any state and "doing business" in New York

Enforcement

- ***Enforcement***
  - Civil actions to recover penalties may be brought by the Attorney General, a district attorney, a city attorney, or a city prosecutor.
- ***Private Right of Action***
  - Civil actions to recover penalties may be brought by a customer.

There are no ***Data Safe Harbors***

There are no ***Vendor Provisions***

Pennsylvania

Consumer Data Privacy Act

- Legislative Status: Referred to Committee on Consumer Affairs; 4/5/2019
- Link to Text: HB 1049

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** is not specifically defined in the statute.

- ***Personal Information*** is defined as information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked to either a particular consumer or household and includes:

  - Identifiers (e.g., name, address, usernames, email addresses, account names, Social Security numbers, driver's license numbers, etc.)

  - Characteristics of protected classifications

  - Commercial information (e.g. records of personal property, products or services purchased, or other purchasing or consuming history)

  - Biometric information

  - Internet activity

- Geolocation data
- Audio/electronic/visual/thermal/olfactory information
- Professional or employment-related information
- Education information; and
- Inferences drawn from any of the above to create a "profile about a consumer" that reflect preferences, psychological trends, behaviors, etc.
- Personal Information does not include publicly available information

- ***Business*** is defined as any for-profit legal entity doing business in Pennsylvania that collects consumers' personal information "or on the behalf of which such information is collected" and determines the purposes and means of processing of consumers' financial information that meets one of these thresholds:
  - Annual Gross Revenue greater than $10 million ($10,000,000)
  - Alone or in combination, buys, receives for a commercial purpose, sells for a commercial purpose the personal information of 50,000+ consumers, households, or devices or
  - Derives 50 percent or more of annual revenues from selling consumers' personal information.
- ***Business*** also includes any entity that controls a business as defined above and shares common branding with the business.

Enforcement

- ***Enforcement***
  - The Attorney General may bring a civil action to recover penalties

- ***Private Right of Action***
  - A consumer may bring a civil action for damages of no less than $100 and no more than $750 per consumer per incident and may seek injunctive or declaratory relief

Data Safe Harbors

- A business or service provider is not required to comply with a consumer's request to delete information if it is necessary for the business/service provider to maintain the consumer's personal information to:
  - Complete the transaction for which the information was collected;
  - Detect security incidents;
  - To identify and repair errors that impair functionality;
  - Exercise free speech;
  - Engage in public or peer-reviewed research;
  - To enable internal uses that are aligned with the expectations of the consumer.
- This law will not restrict a business's ability to comply with the law; civil/criminal/or regulatory inquiry; cooperate with law enforcement; exercise/defend legal claims; collect/use/retain/sell or otherwise disclose de-identified data; or collect or sell a consumer's personal information if every aspect of the commercial conduct occurs outside Pennsylvania

Vendor Provisions

- A third party shall not sell personal information about a consumer that was sold to the third party by a business unless the consumer received explicit notice and provided an opportunity to opt out.

Washington

Washington Privacy Act

- Legislative Status: Returned from House of Representatives to Senate Rules Committee in April 2019 for third reading.
- Effective Date: N/A
- Link to Text: SB 5376

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction	✓	

Key Definitions

- ***Consumer*** means a natural person who is a Washington State resident acting only in an individual or household context.

  Consumer does not include a natural person acting in a commercial or employment context.

- ***Personal Data*** means any information that is linked or reasonably linkable to an identified or identifiable natural person.

  Personal Data does not include de-identified data or publicly available information (information that is lawfully made available from federal, state, or local government records.)

- ***Business*** is not defined by the bill. However, it defines the jurisdictional scope of the bill as applicable to legal entities that conduct business in Washington, or produce products

or services that are intentionally targeted to residents of Washington, and that satisfy one or more of the following thresholds:

- Controls or processes personal data of 100,000 consumers or more; or
- Derives over 50 percent of gross revenue from the sale of personal data and processes or controls personal data of 25,000 consumers or more."

- A data ***Controller*** is a natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- A data ***Processor*** is a natural or legal person that processes personal data on behalf of the controller. Processing is governed by a contract between the controller and the processor that sets out the processing instructions to which the processor is bound.

Enforcement

- ***Enforcement***
  - The Washington Attorney General may bring an action either in the name of the state, or as *parens patriae* on behalf of persons residing in the state, to enforce the bill.

- ***Private Right of Action***
  - There is no private right of action.

Data Safe Harbors

- The bill does not apply to:
  - State and local governments;
  - Municipal corporations;
  - Information that meets the definition of[1]:
    - Protected Health Information under HIPAA
    - Health care information for purposes of 70.02 RCW

[1] The limitations set forth in this bullet point also apply to information maintained by a covered entity or business associate as defined by HIPAA; a health care facility or health care provider as defined by RCW 70.02.010; or a program or qualified service organization as defined by 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290 dd-2.

- Patient identifying information for purposes of 42 C.F.R. Part 2;
- Identifiable private information for purposes of the federal policy for the protection of human subjects
- Information and documents created specifically for, and collected and maintained by: a quality improvement committee, a peer review committee, a quality assurance committee, a hospital for reporting of health care-associated infections, a notification of an incident, or reports regarding adverse events;
- Information and documents created for purposes of the federal health care quality improvement act of 1986, and related regulations; or
- Patient safety work product information for purposes of 42 C.F.R. Part 3

➢ Personal data provided to, from, or held by a consumer reporting agency where such use is in compliance with the federal fair credit reporting act

➢ Personal data collected, processed, sold, or disclosed pursuant to the GLBA;

➢ Personal data collected, processed, sold or disclosed pursuant to the federal driver's privacy protection act of 1994, where such use is in compliance with the law.

➢ Data maintained for purposes of employment records.

❖ The obligations set forth in the bill do not restrict a controller's or processor's ability to:

➢ Comply with federal, state, or local laws, rules, or regulations;

➢ Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;
➢ Cooperate with law enforcement agencies;
➢ Investigate, exercise, or defend legal claims;

➢ Prevent or detect identity theft, fraud, or other criminal activity or verify identities;

- Perform a contract to which the consumer is a party or in order to take steps at the request of the consumer prior to entering into a contract;
- Protect the vital interests of the consumer or of another natural person;
- Perform a task carried out in the public interest or in the exercise of official authority vested in the controller;
- Process personal data of a consumer for one or more specific purposes where the consumer has given their consent to the processing; or
- Prevent, detect, or respond to security incidents or investigate, report or prosecute those responsible for any such action.

❖ The consumer's right to deletion does not apply to the extent processing is necessary:

- For exercising the right of free speech;
- For compliance with a legal obligation that requires the processing of personal data or for the performance of a task carried out in the public interest/health or in the exercise of official authority vested in the controller;
- For archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, where the deletion of such personal data is likely to render impossible or seriously impair the achievement of the objectives of the processing;
- For the establishment, exercise, or defense of legal claims;
- To detect or respond to security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or identify, investigate, or prosecute those responsible for that activity; or
- For a data broker that received the personal data from third parties and is acting as a controller, solely to prevent the personal data from reappearing in the future.

Vendor Provisions

- There are no provisions specifically addressing vendors.

BILLS THAT WERE RELEGATED TO PROMOTE STUDIES ON DATA PRIVACY LAWS

Connecticut
Louisiana
Missouri
North Dakota
Rhode Island