CYBERLAW CLINIC
HARVARD LAW SCHOOL | BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY

MEMORANDUM

To: Representative Stephanie Jerome

From: Harvard Cyberlaw Clinic

Date: January 5, 2024

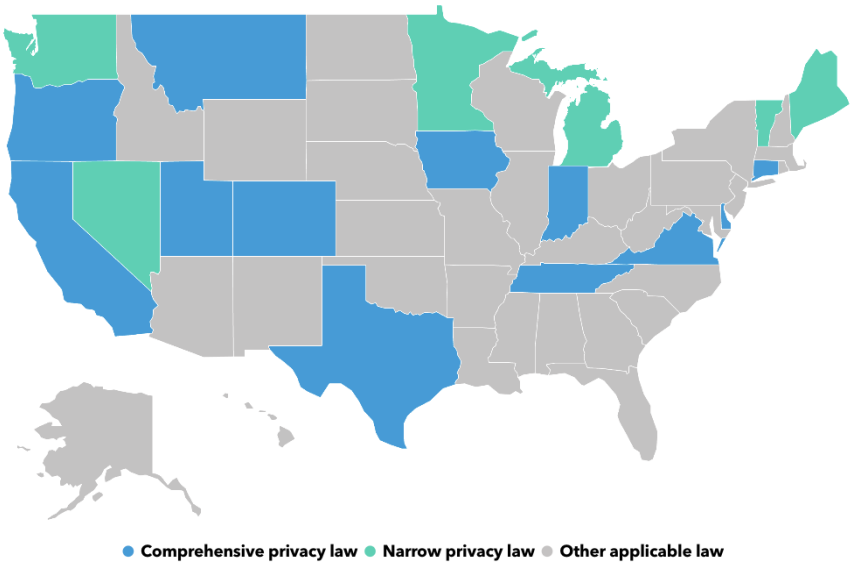
Re: State Data Privacy Frameworks

1. OVERVIEW

Privacy laws in the U.S. have historically been sector-specific, covering narrow types of personal data such as health information or student records. However, recent developments have seen a trend toward comprehensive state-level privacy legislation. For the purposes of this analysis, "comprehensive data privacy laws" are non-sector-specific laws intended to create broad fundamental data privacy rights, principles and requirements.

Thirteen states – California, Virginia, Colorado, Connecticut, Utah, Iowa, Indiana, Tennessee, Texas, Florida, Montana, Oregon, and Delaware – currently have comprehensive data privacy laws. During the 2022-23 legislative cycle, twelve states– Illinois, Louisiana, Massachusetts, Minnesota, New Hampshire, New Jersey, New York, North Carolina, Oklahoma, Pennsylvania, Rhode Island and Vermont – introduced bills addressing privacy issues like biometric identifiers and health data protection.

The implementation of comprehensive privacy legislation differs from state to state. For example, some states, like California and Connecticut, grant consumers additional rights to limit the use and disclosure of sensitive personal information. States also differ on enforcement, with California providing enforcement though a specialized agency, and all others providing enforcement through a state attorney general and/or private rights of action.



Graphic sourced from Bloomberg Law: https://infogram.com/data-privacy-map-4-2023-1hxr4zx19z97q6y.

This section compares the broad structure of the data privacy protection frameworks of three states of particular interest: California, Connecticut, and Montana. It then provides recommendations for how Vermont can incorporate the best elements of these laws.

2. DATA PRIVACY FRAMEWORKS ACROSS STATES

2.1. California (CPPA and CPRA)

2.1.1. Background

California's data privacy protection laws are primarily embodied in two acts: the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), an expansion of the CCPA. CCPA and CPRA came into effect in 2020 and 2023, respectively.

The CCPA was introduced as the first comprehensive data privacy law in the U.S. It governs how companies should handle private data and how consumers can exercise their data privacy rights.

The CPRA expands on the CCPA with provisions regarding sensitive data, consumer rights, data minimization, and purpose limitation, and it introduces a new Privacy Enforcement Authority. It superseded any areas of conflict with the CCPA on January 1, 2023.

2.1.2. Key Definitions

Covered Business: The CCPA and CPRA only apply to covered businesses. Covered businesses are for-profit entities that meet one of the following criteria:

1. gross annual revenue of over $25 million;
2. buys, sells or shares personal information of 100,000 or more California residents or households; or
3. derives 50% or more of annual revenue from selling or sharing California personal information.

The following entities are specifically not covered businesses, and therefore exempt under the CCPA and CPRA: nonprofits, government agencies, and institutions and data that are already subject to federal data privacy laws, such as the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act (HIPAA)

Personal Information: The CCPA and CPRA governs use of personal information. Personal information is 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. The CCPA identifies eleven categories of personal information:

1. **Identifiers**: Name, alias, postal address, unique personal identifier, online identifier, Internet Protocol (IP) address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
2. **Customer records information**: Name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit or debit card number, other financial information, medical information, health insurance information.
3. **Characteristics of protected classifications under California or federal law**: Race, religion, sexual orientation, gender identity, gender expression, and age.
4. **Commercial information**: Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
5. **Biometric information**: Hair color, eye color, fingerprints, height, retina scans, facial recognition, voice, and other biometric data.
6. **Internet or other electronic network activity information**: 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. **Professional or employment-related information**
10. **Education information**: Information that is not "publicly available personally identifiable information" as defined in the California Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
11. **Inferences**

The CCPA does not restrict currently a business's ability to collect, use, retain, sell, or disclose consumer information that is de-identified or aggregated.

Sensitive Information: Some provisions of the CPRA only apply to provide extra protection for specific categories of sensitive personal information. Sensitive Information includes the following categories:

1. Social Security numbers (SSNs),
2. Driver's license,
3. Financial account or card numbers,
4. Precise geolocation,
5. Racial and ethnic characteristics,
6. Religious and philosophical beliefs,
7. Union membership,
8. Contents of mail, email, and text messages,
9. Genetic and biometric data.

2.1.3. Obligations of Covered Entities

Notice: Businesses must inform consumers of the categories of personal data they collect and the purposes for which they will use it. This information must be provided before the data is collected. They must also notify users before selling or sharing data with third parties, detailing which categories are involved and the buyers or recipients of the data.

Consent: Explicit consent to collect, use, or sell personal data about adults is not generally required. However, consumers have the right to know what data is collected and sold, and the right to prohibit the sale of their data. Businesses can't refuse service or charge more to people who exercise these rights. A dedicated "Do Not Sell My Personal Information" page must be provided for consumers to exercise their opt-out rights.

Selling or sharing the personal data of individuals under 16 requires active, advanced consent. For those between 13 and 16, consent from the individual is required, and for those under 13, consent from a parent or guardian is needed.

Data Minimization: Collection, use, retention, and sharing of a consumer's personal information must be:

1. Reasonably necessary and proportionate to achieve the purposes for which the information was collected.
2. Compatible with the context in which the personal information was collected.
3. Not further processed in a manner that is incompatible with those purposes.

The processing of consumer personal information must meet the reasonable expectations of consumers based on factors like the relationship with the business and the type of personal information collected. Furthermore, businesses must ensure that they obtain only the minimum amount of personal information required to accomplish a processing purpose, assess the

potential risks to consumers from data collection and processing, and implement additional protections to address identified risks.

2.1.4. Consumer Rights

In addition to the obligations placed on covered businesses, the CCPA and CPRA give consumers rights that they can affirmatively invoke. Consumer data privacy rights include:

- Right to know and access
- Right to deletion
- Right to opt-out of sale of data and sharing for cross-context behavioral advertising
- Right to nondiscrimination
- Right to data portability
- Right to rectification and correction
- Right to limit use and disclosure of sensitive personal information
- Right to opt-out of the use of automated decision-making
- Extra protections for minors under the age of 16, and especially under the age of 13

2.1.5. Compliance

Covered businesses must publish and maintain a compliant privacy policy which is updated at least once every 12 months. Privacy policies must include:

- Contact Information: Provide clear contact information, including a toll-free telephone number and online contact details for consumers to exercise their rights.
- Do Not Sell My Information Page: If selling personal information, provide an opt-out page linked clearly on the business's homepage or website footer.
- Right to Opt-Out of Marketing: Notify customers if their data is used for marketing or sold to third parties and provide them with the option to opt out.

If consumers make a data access request, businesses must provide details about the data collected, the reasons for using the data, and with whom it has been shared, covering the past 12 months. Consumers may request the deletion of some of this data unless it's needed for an ongoing contract, transaction, or for security reasons. Businesses must confirm receipt of a deletion request within 10 business days respond to requests to delete within 45 calendar days. This response period may be extended by an additional 45

days when reasonably necessary, so long as the business informs the consumer of any such extension within the initial 45-day response period.

Consumers have the right to opt out of the sale of their personal data. Businesses must comply within 10 days and cannot request reauthorization for at least 12 months. They must also inform any third parties they have sold data to, who must also cease selling the data.

2.1.6. Enforcement

In California, the enforcement of data privacy laws is primarily executed by the California Privacy Protection Agency (CPPA). Established with the introduction of the CPRA, the CPPA has full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act (CCPA) and the CPRA. The agency is responsible for investigating potential violations and initiating actions through the Administrative Law Court. This marks a change from the CCPA, where enforcement actions were previously initiated through state court. However, enforcement by the state Attorney General is still permitted. Enforcement through private actions is generally not permitted, except to allow consumers to sue for a data breach under specific circumstances. Entities or individuals that violate the CCPA/CRPA may receive a maximum civil penalty of $2500 if the violation is found to be unintentional, and $7500 if the violation is found to be intentional.

2.2. Connecticut (CTDPA)

2.2.1. Background

The Connecticut Data Privacy Act (CTDPA) became effective July 1, 2023, making Connecticut the fifth state to enact comprehensive data privacy laws, after California, Virginia, Colorado and Utah. Of its predecessors, CTDPA is most like the consumer rights-oriented Virginia Consumer Data Privacy Act (VCDPA) and Colorado Privacy Act (CPA) than the more business-friendly Utah Consumer Privacy Act (UCPA). Many states which have enacted comprehensive data privacy laws after the CTDPA, like Montana, have closely mirrored the CTDPA's definitions, structure, and enforcement mechanisms.

2.2.2. Key Definitions

Controllers: The CTDPA applies data privacy regulations to controllers, which are organizations or persons that conduct business in Connecticut or produce products or services targeting Connecticut residents, and which over the course of a calendar year:

1. Controlled or processed Personal Data of at least 100,000 Consumers, excluding Personal Data controlled or processed for the purpose of completing a payment transaction; or
2. Controlled or processed the Personal Data of at least 25,000 Consumers and derived more than 25% of their gross revenue from the sale of Personal Data.

CTDPA exempts institutions and data that are already subject to the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act. The CTDPA also does not apply to several other kinds of businesses and data, such as nonprofit entities, many schools, and consumer reports.

Consumers: The CTDPA provides certain rights to consumers, who are defined as residents of the state not acting in an employment or commercial context.

Personal Data: The CTDPA governs personal data, which is any information that is linked or reasonably linkable to an identified or identifiable individual. Personal data does not include de-identified data or publicly available information.

Sensitive Data: Certain provisions of the CTDPA apply only to sensitive data. Sensitive data is personal data that reveals racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, citizenship, or immigration status; the processing of genetic or biometric data for the purpose of uniquely identifying an individual; personal data collected from a known child (i.e., under age 13); or precise geolocation data.

Targeted Advertising: The CTDPA specifically regulates targeted advertising using personal data. Targeted advertising means displaying to a consumer an advertisement that is selected based on personal data obtained or inferred over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict consumer preferences or interests. It does not include, among other things, advertisements based on activities within a controller's own websites or online applications, or the context of a consumer's current search query, visit to a website, or online application.

2.2.3. Obligations of Covered Entities

Notice: Privacy notices must be clear, accessible, and meaningful, detailing categories of personal data processed, purposes of processing, how consumers can exercise their rights, how to appeal decisions, and third-party sharing information.

Consent: Controllers may not process sensitive personal data without obtaining a consumer's consent. Nor may controllers process personal data for purposes not previously disclosed, unless the controller first obtains the consumer's consent.

The CTDPA prohibits the use of dark patterns (i.e. any user interface that the Federal Trade Commission would identify as a dark pattern) that impair user autonomy, decision-making, or choice, and any consent obtained through dark patterns is invalid. Controllers are subject to stringent protections for minors' data, aligning with regulations like the Children's Online Privacy Protection Rule for those under 13.

Data Minimization: Controllers may collect only the minimum amount of personal data necessary for the purposes for which they are collected. Moreover, controllers can only use personal data for the purposes that have been disclosed to the consumer through a privacy notice.

2.2.4. Consumer Rights

The CTDPA provides residents with several rights regarding their personal data. These rights include:

- The right to confirm if their personal data is being processed and to access their data.
- The right to correct inaccuracies in their personal data.
- The right to have their personal data deleted.
- The right to data portability, allowing them to get a copy of their personal data in a portable format.
- The right to opt-out of targeted advertising, the sale of personal data, and profiling in automated decision-making that has legal or similar effects.
- Protection against discrimination for exercising their data privacy rights.
- Extra protections for minors
- Extra protections for sensitive data

2.2.5. Compliance

Organizations must respond to consumer requests within 45 days, with a possible extension of an additional 45 days.

Organizations are required to conduct data protection assessments for processing activities that present heightened risks to consumers, such as targeted advertising, profiling, and the sale of personal data. The assessments

should weigh benefits against potential risks, considering the use of de-identified data, consumer expectations, the processing context, and the organization-consumer relationship. Controllers must also establish, implement, and maintain reasonable administrative, technical, and physical practices to protect the confidentiality, integrity, and accessibility of Personal Data, appropriate to the volume and nature of the data at issue. These assessments may be requested by the Attorney General for investigations.

2.2.6. Enforcement

The Connecticut Attorney General is the exclusive enforcer of the CTDPA, with the authority to issue monetary and administrative sanctions. Organizations have a 60-day cure period to address violations, after which penalties may be imposed. Entities or individuals that violate the CTDPA may face civil penalties up to $5,000 per violation. No private right of action is provided under the CTDPA.

2.3. Montana (MCDPA)

2.3.1. Background

The Montana Consumer Data Privacy Act (MCDPA) is Montana's data privacy protection legal framework. It passed in April 2023 and is set to go into effect in October 2024.

Montana is the ninth state to pass comprehensive state data privacy laws, and broadly mirrors Connecticut's CTDPA in structure and purpose.

2.3.2. Key Definitions

Personal data: The MCDPA defines personal data as any information that is linked or reasonably linkable to an identified or identifiable individual. This excludes deidentified data or publicly available information.

Controller: The MCDPA applies to controllers, or any company that:

- conducts business in Montana or provides goods or services to Montana consumers, and
- either:
    - controls or processes personal data of 50,000 or more Montana consumers, or
    - controls or processes personal data of 25,000 or more Montana consumers and derives more than 25% of its gross revenue from selling that data.

MCDPA contains exemptions for certain categories of entities, similar to other comprehensive state privacy laws. The excluded categories under the MCDPA include:

- Governmental entities
- Financial institutions governed by the Gramm-Leach-Bliley Act
- Covered entities and business associates subject to the Health Insurance Portability and Accountability Act
- Non-profit organizations
- Institutions of higher education

Sensitive Data: The MTCDPA restricts the collection and processing of "sensitive data" without consent. The MTCDPA defines "sensitive data" as:

1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation citizenship and immigration status;
2. Genetic and biometric data that identifies an individual;
3. Precise geolocation data (location within a radius of 1,750 feet);
4. Personal data collected from a known child (i.e., someone under the age of 13).

2.3.3. Obligation of Covered Entities

Notice: Controllers must provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes the categories of personal information processed, the purpose for processing personal information, any categories of personal data that the controller shares with third parties, the categories of any third parties with whom the controller shares personal data, a means that the consumer may use to contact the controller (such as an active email address), and how consumers may exercise their data privacy rights.

Consent: Like in Virginia, Connecticut and Colorado, controllers may not process sensitive personal data without obtaining a consumer's consent. Nor may controllers process personal data for purposes not previously disclosed, unless the controller first obtains the consumer's consent. Consumers may revoke consent at any time. Controllers must obtain consent from the parents of children under the age of 13.

Data minimization: Controllers may collect only the minimum amount of personal data necessary for the purposes for which they are collected. Moreover, controllers can only use personal data for the purposes that have been disclosed to the consumer through a privacy notice.

2.3.4. Consumer Rights

Under the MCDPA, consumers have the right to:

- know when their personal data is being processed
- access their personal data
- correct or amend their personal data
- delete their personal data
- opt out of the processing of their personal data for targeted advertising or the sale of their personal data
- be free from discrimination for exercising these rights

2.3.5. Compliance

As provided in other state privacy laws, controllers must respond to consumer requests to exercise their data privacy rights within 45 days (with a 45-day extension available, if "reasonably necessary") and must offer consumers the right to appeal an adverse decision. The appeal response must be delivered by a controller to a consumer within 60 days, and if controllers deny an appeal, as in Virginia, controllers must provide a consumer with a method for contacting the attorney general to submit a complaint.

Like its counterpart laws in Virginia, Connecticut, and Colorado, the MTCDPA requires controllers to conduct data protection assessments for processing activities which present a heightened risk of harm. Such activities include processing personal data for targeted advertising, sale of personal data, processing sensitive data and processing of personal information for profiling if the profiling presents a reasonably foreseeable risk of unfair or deceptive or unlawful disparate impact on consumers, "intrusion upon seclusion," or other financial, reputational, or physical harms.

These assessments must outline the balance between the advantages for controllers and the potential risks to consumer rights, detailing any protective measures. Assessments in compliance with other states' data privacy laws that align in scope and effect with Montana's will be accepted.

2.3.6. Enforcement

The MCDPA creates an opt-in requirement for processing the personal data of minors which aligns with similar protections in California's and Connecticut's privacy laws.

Enforcement of the MCDPA is solely executed by the Montana Attorney General. If a business is found to be in violation of the Act, the Montana Attorney General may issue a notice. If the business fails to cure the violation

within a 60-day cure period, the Attorney General may bring an action against it. No private right of action is provided under the MCDPA.

3. EXCEPTIONS TO DATA PRIVACY REGULATIONS

Existing comprehensive state data privacy laws often do not extend to data covered by federal data privacy laws (e.g. Fair Credit Reporting Act, Gramm-Leach-Bliley Act, FERPA and HIPAA), and often exempt state and local government agencies and non-profit organizations. Furthermore, irrespective of the collecting or processing entity, certain data types like employee and HR data (with California's CPRA as an exception), deidentified data, and publicly available information are typically excluded from these privacy regulations.

3.1. State and local governmental agencies

While all federal governmental agencies are excluded from state privacy laws due to federal preemption of state laws, most states like California, Connecticut, Montana, Indiana, Iowa and Virginia specifically exempt state and local governmental agencies as well. Not all states follow this mold, however, as other states like Alabama and Delaware include such agencies within the ambit of their privacy regulations.

3.2. Nonprofits

Connecticut, Florida, Indiana, Iowa, Montana, Tennessee, Texas, Utah, Virginia wholly exempt non-profits from their data privacy regulations, although their legal definitions vary, affecting the scope of exemption. However, political organizations are generally not exempt under the state privacy laws. Currently, only Texas and Virginia contain an express exemption directed to political organizations.

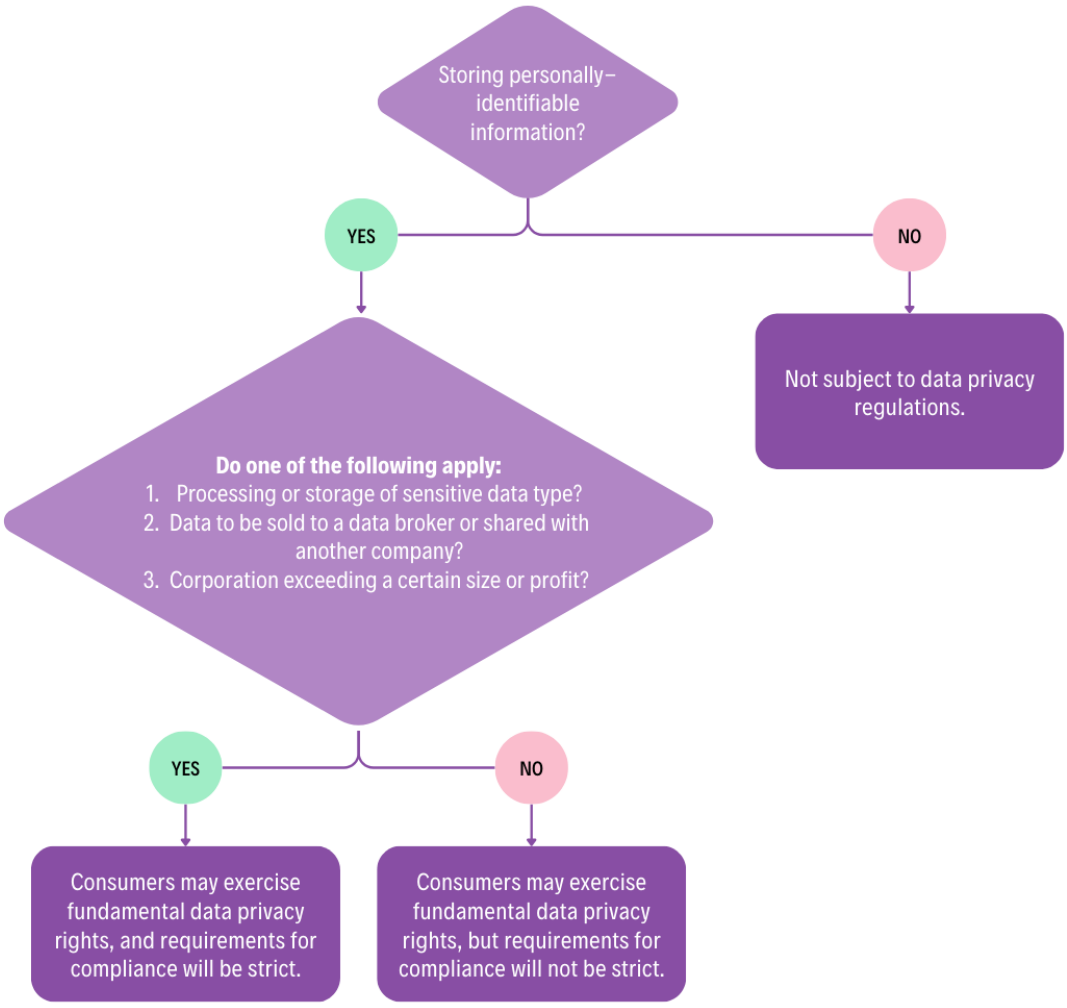
Several states have deviated from the norm of exempting non-political nonprofits. Delaware and Nevada's data privacy laws wholly subject nonprofits to their data privacy regulations. Colorado's data privacy laws apply to non-profits that engage in commerce or offer commercial products/services within the state, subject to data processing or revenue criteria. California generally exempts non-profits from their data privacy protection laws, but applies its requirements to non-profits when they qualify as "service providers," "contractors," or "third parties." Delaware and Oregon grant exemptions only to non-profits involved in particular missions, such as combating insurance crime or fraud, with Oregon also exempting non-commercial media activities.

4. RECOMMENDATIONS FOR VERMONT

Our recommendation for Vermont is to largely follow the trend of states enacting data privacy regulations very similar to Connecticut's CTDPA.

We recommend Vermont largely establish the same definitions for personal information and sensitive information as the CTDPA, as well as establish the same set of fundamental data privacy rights (e.g. the right to delete personal information, the right to receive notice of personal information, etc.). This means deidentified data and publicly-available information would not be covered under these definitions. Vermont may choose include state and local government agencies and nonprofits within its framework.

We recommend a compliance structure which is modified from the CTDPA. The intent of such a modified structure would be to lessen the compliance cost for small Vermont businesses not engaging in high-risk data practices (i.e. the collection or processing of sensitive information and the sale of data). Such a framework would provide stricter requirements for covered controllers to comply with consumer requests when controllers (1) stored or processed sensitive personal information, (2) sold personally identifiable information to data brokers or otherwise shared such information beyond their corporate governance structure, or (3) exceeded a certain size or profit. This framework is detailed in the chart below:



Under this framework, the obligation of covered entities for notice, consent and data minimization would be the same for all controllers collecting or storing personally-identifiable information, but small businesses not engaging in high-risk data practices would have extended periods of time to respond to consumer requests (e.g., 60 days instead of 45 days) and smaller fines for noncompliance (e.g., $1,000 instead of $5,000).

5. SOURCES

Bloomberg Law. "California Consumer Privacy Laws: CCPA & CPRA." https://pro.bloomberglaw.com/brief/california-consumer-privacy-laws-ccpa-cpra/.

Davis Wright Tremaine LLP. "Montana Consumer Data Privacy Law." https://www.dwt.com/blogs/privacy--security-law-blog/2023/05/montana-consumer-data-privacy-law.

International Association of Privacy Professionals (IAPP). "Exceptions in New State Privacy Laws Leave Data Without Security Coverage." https://iapp.org/news/a/exceptions-in-new-state-privacy-laws-leave-data-without-security-coverage/.

International Association of Privacy Professionals (IAPP). "Filling the Void: The 2023 State Privacy Laws and Consumer Health Data." https://iapp.org/news/a/filling-the-void-the-2023-state-privacy-laws-and-consumer-health-data/.

Morrison & Foerster LLP. "Connecticut to Enact a Comprehensive Consumer Privacy Law." https://www.mofo.com/resources/insights/220519-connecticut-enact-a-comprehensive-consumer-privacy-law.

Venable LLP. "What Nonprofits Need to Know About State Privacy Laws." https://www.venable.com/insights/publications/2023/10/what-nonprofits-need-to-know-about-state.

White & Case LLP. "Delaware Comprehensive Data Privacy Law." https://www.whitecase.com/insight-alert/delaware-comprehensive-data-privacy-law.

WireWheel. "CCPA and CPRA: California Data Privacy Law Guide." https://wirewheel.io/blog/ccpa-and-cpra-california-data-privacy-law-guide/.