THE DEVIL IS IN THE DETAILS: KEY DIFFERENCES IN U.S. DATA PRIVACY LAWS

M. Lynne Hewitt

Aviva Surugeon

The regulatory landscape surrounding data privacy is changing rapidly, with individual states adopting new legislation to address constituents' privacy concerns in the absence of an overarching federal law. So far, five states have enacted comprehensive privacy laws: California, Colorado, Connecticut, Utah, and Virginia. The California Consumer Privacy Act (CCPA) has been in effect since 2020. The California Privacy Rights Act (CPRA), which amends and expands the CCPA, Colorado Privacy Act (CPA), Connecticut Data Privacy Act (CTDPA), Utah Consumer Privacy Act (UCPA), and Virginia Consumer Data Protection Act (VCDPA) will all take effect in 2023. While all these privacy laws impose requirements on covered businesses regarding the collection and use of consumers' personal information, the laws are distinct, and understanding their nuances is crucial to ensure compliance across state lines.

Common Themes

There are many similarities among these new privacy laws. For example, covered businesses in all five states will be required to:

- Be transparent and provide notice to consumers;
- Limit their processing of personal information;
- Refrain from discriminating against consumers who exercise their rights; and
- Perform data protection assessments.

Further, consumers in all five states will have rights of:

- Access;
- Rectification;
- Deletion;
- Portability; and
- Opting out of certain transactions.

Little Details Make a Big Difference

Despite their commonalities, significant differences will exist between the five States' laws when they each become fully effective. These include, but are not limited to, differences in:

- Key definitions;
- Scope;
- Exemptions; and
- Administration and enforcement.

When viewed more in-depth, all five laws broadly define the term "personal information" or "personal data." Unlike the CCPA, however, the CPA, VCDPA, UCPA, and CTDPA

borrow terms and definitions from the EU General Data Protection Regulation (GDPR), such as "controller" and "processor" when referring to covered entities and their service providers, respectively, and "personal data." In addition, the CPA, VCDPA, and CTDPA require covered entities to conduct data security assessments for data processing activities that present a "heightened" risk of harm, such as profiling, selling personal data, processing sensitive personal data, and engaging in targeted advertising.

Unlike the CCPA, which allows a private right of action for breaches of personal information, neither the CPA, VCDPA, UCPA, or CTDPA includes a private right of action for any type of violation. The CPRA extends the CCPA private right of action to data breaches that compromise a username and password and creates a new regulatory and enforcement body, the California Privacy Protection Agency. In contrast, the VCDPA grants enforcement authority solely to the Attorney General. The UCPA provides for a bifurcated enforcement scheme. First, the Utah Department of Commerce Division will investigate companies based on consumer complaints, and it then sends cases it deems legitimate to the Attorney General's office. Then, before initiating enforcement action, the Attorney General must first provide the business with (1) written notice 30 days before and (2) an opportunity to cure within 30 days of receipt of the notice.

The attached chart provides a high-level comparison of some of the key features of each state law.

Preparation will be the key to avoiding issues with compliance and claims of alleged violations. Organizations must review each law in detail to assess the proper application and compliance required. Also, states like California and Colorado have only begun the rulemaking process under their respective statutes, meaning that new or different substantive obligations may yet be forthcoming. Redgrave, LLP will continue to monitor the changing landscape of U.S. data privacy legislation and are available to consult and assist in the development and deployment of successful information governance and privacy policies and practices.

For additional information on this topic or further details on Redgrave LLP's Data Privacy services, please contact **Martin Tully** at mtully@redgravellp.com or at 773.782.0352 .

Redgrave LLP *is one of the largest legal practices focused exclusively on addressing the legal challenges that arise at the intersection of the law and technology, including eDiscovery, information governance, and data privacy. We employ some of the most experienced professionals in the field. We provide clients with practical, innovative, and cost-effective solutions and serve Global and Fortune 500 companies across a diverse array of industries. We also work collaboratively with Am Law 100 law firms in roles ranging from co-counsel to consulting and testifying expert witnesses and have appeared in state and federal courts throughout the United States.*

	CCPA	CPRA	VCDPA	CPA	UCPA	CTDPA
When does it take effect?						
	Jan. 1, 2020	Jan. 1, 2023	Jan. 1, 2023	July 1, 2023	Dec. 31, 2023	July 1, 2023
What types of data are protected?						
Statutory Term	Personal information	Personal information	Personal data	Personal data	Personal Data	Personal Data
Defined	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	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	Any information that is linked or reasonably linkable to an identified or identifiable natural person	Information that is linked or reasonably linkable to an identified or identifiable individual	Information that is linked or reasonably linkable to an identified or identifiable individual	Information that is linked or reasonably linkable to an identified or identifiable individual
Who must comply with each data privacy law?						
Jurisdictional Threshold	"Does business" in California	"Does business" in California	"Conduct business" in Virginia or produce products or services "targeted" to Virginia residents	"Conducts business" in Colorado or produces or delivers commercial products or services "intentionally targeted" to Colorado residents	"Conducts business" in Utah or targets products and services to consumers who are Utah residents	"Conducts business" in Connecticut or targets products and services to consumers who are Connecticut residents
Revenue Threshold	Annual gross revenues greater than $25 million	Annual gross revenues greater than $25 million in the preceding calendar year	None	None	Annual gross revenues greater than $25 million	None

	CCPA	CPRA	VCDPA	CPA	UCPA	CTDPA
Processing Threshold	Data of 50,000 or more consumers	Data of 100,000 or more consumers	Data of 100,000 or more consumers	Data of 100,000 or more consumers	Data of 100,000 or more consumers	Data of 100,000 or more consumers
What type of data and entities are exempt?						
Data Exemptions *(This information is not meant to be comprehensive. Please refer to actual laws for more in-depth information on data exemptions)*	Personal information collected and used outside the state of CA, certain employment information, Information subject to and governed by, HIPPA, GLBA, the Fair Credit Reporting Act, the Driver's Privacy Protection Act, the Family Educational Rights and Privacy Act, and the Farm Credit Act.	Adds "share" to the definition from CCPA as it relates to conduct that takes place wholly outside of California. Additional data exemptions mirror CCPA with the exception of Section 1794.146 because it was a September 2020 amendment to the CCPA	Information subject to and governed by, HIPPA, GLBA, the Fair Credit Reporting Act, the Driver's Privacy Protection Act, the Family Educational Rights and Privacy Act, and the Farm Credit Act.	Information subject to and governed by, HIPPA, GLBA, the Fair Credit Reporting Act, the Driver's Privacy Protection Act, the Family Educational Rights and Privacy Act, and the Farm Credit Act.	Information subject to and governed by, HIPPA, GLBA, the Fair Credit Reporting Act, the Driver's Privacy Protection Act, the Family Educational Rights and Privacy Act, and the Farm Credit Act.	Information subject to and governed by, HIPPA, GLBA, the Fair Credit Reporting Act, the Driver's Privacy Protection Act, the Family Educational Rights and Privacy Act, and the Farm Credit Act.
Entity Exemptions	Applies only to for-profit organizations	Applies only to for-profit organizations	Excludes any governmental entity or a third party working on behalf of a governmental entity; an institution of higher education; financial institution subject to Gramm-Leach-Bliley Act; a nonprofit corporation; a covered entity and business associate under HIPAA	Excludes any governmental entity or a third party working on behalf of a governmental entity; an institution of higher education; financial institution subject to Gramm-Leach-Bliley Act; a nonprofit corporation; a covered entity and business associate under HIPAA	Excludes any governmental entity or a third party working on behalf of a governmental entity; a tribe; an institution of higher education; a nonprofit corporation; a covered entity and business associate under HIPAA	Excludes any governmental entity or a third party working on behalf of a governmental entity; an institution of higher education; financial institution subject to Gramm-Leach-Bliley Act; a nonprofit corporation; a covered entity and business associate under HIPAA

	CCPA	CPRA	VCDPA	CPA	UCPA	CTDPA
What constitutes the sale of personal data?						
Defined	Selling, renting, releasing, disclosing, disseminating, making available, transferring, or communicating personal information for monetary or other valuable consideration	Adds "sharing" to the definition from CCPA and clarifies that behavioral advertising constitutes a sale	Exchange of personal data for monetary consideration	Exchange of personal data for monetary or other valuable consideration	Exchange of personal data for monetary or other valuable consideration	Exchange of personal data for monetary or other valuable consideration
How is the law to be enforced?						
	Enforcement and rulemaking by state Attorney General with 30-day cure period for alleged violations Limited private right of action	New California Privacy Protection Agency (CPPA), charged with enforcement and rulemaking Limited private right of action	Enforcement by state Attorney General No private right of action	State Attorney General charged with implementing and enforcing the CPA, including adopting new rules No private right of action	Enforcement by state Attorney General with 30-day cure period for alleged violations No private right of action	Enforcement by state Attorney General with 60-day cure period (until 12/31/24) No private right of action