The Biggest Year Yet for US Privacy Laws is Around the Corner

By: Billee McAuliffe, Melissa Powers, and Cassidy Kolaz of Lewis Rice LLC

2023 is proving to be an important year in the privacy world. As of July 2022, five states - California, Virginia, Colorado, Utah and Connecticut - have enacted comprehensive privacy laws designed to increase protections for consumers' personal data and provide consumers with certain rights to control their personal data. California's law, the California Consumer Rights Act of 2020 (CPRA), which amends the California Consumer Privacy Act of 2018 (CCPA), and Virginia's law, the Virginia Consumer Data Protection Act (VA CDPA), each will take effect January 1, 2023. Colorado's law, the Colorado Privacy Act (ColoPA), and Connecticut's law, the Connecticut Act Concerning Personal Data Privacy and Online Monitoring (CT DPA), will both take effect July 1, 2023. Utah's law, the Utah Consumer Privacy Act (UCPA), will take effect December 31, 2023.

Applicability

The first question to consider is whether these laws apply to your business. As each of the laws have different jurisdictional criteria, the answer may vary by state.

The CPRA applies to for-profit entities doing business in California that collect or process personal information of California residents and meet at least one of the following thresholds: (1) yield annual gross revenue in excess of $25 million in the preceding calendar year; (2) annually buy, sell or share personal information of 100,000 or more California residents or households; or (3) derive 50% or more of their annual revenue from selling or sharing California residents' personal information.

Unlike the CPRA, the ColoPA, VA CDPA, and CT DPA do not include a revenue threshold. Rather, the ColoPA applies to persons conducting business in Colorado or producing products or services intentionally targeted to Colorado residents and either: (1) control or process the personal data of 100,000 Colorado residents or more during a calendar year, or (2) derive revenue or receive a discount on the price of goods and services from the sale of personal data and process or control the personal data of 25,000 Colorado residents or more.

Somewhat similarly, the CT DPA applies to persons who conduct business in Connecticut or produce products or services targeted to Connecticut residents during the preceding calendar year and either: (1) control or process personal data of at least 100,000 Connecticut residents, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or (2) control or process personal data of at least 25,000 Connecticut residents and derive over 25% of its gross revenue from the sale of personal data.

Likewise, the VA CDPA applies to persons who conduct business in Virginia or produce products or services targeted to Virginia residents and either: (1) control or process personal data of at least 25,000 Virginia residents; or (2) derive more than 50% of its gross revenue from the sale of personal data.

The UCPA essentially combines the thresholds in the CPRA, VA CDPA, and ColoPA and applies to persons who conduct business or produce products or services targeted to Utah residents, have annual revenue of at least 25 million, and either: (1) control or process personal data of 100,000 or more Utah residents per calendar year; or (2) derive over 50% of its gross revenue from the sale of personal data and control or process the personal data of at least 25,000 Utah residents.

Each law exempts from compliance certain types of entities (e.g., governmental entities, financial institutions governed by the Gramm-Leach-Bliley Act, HIPAA covered entities, and institutions of higher education) and certain types of information (e.g., protected health information).

It is also important to mention that, while your business may not fall within any of the foregoing jurisdictional provisions, if you provide services for other businesses or if you collect or use personal information on behalf of other businesses, you may still need to comply with these laws as a "service provider" or "processor" to regulated entities.

Key Definitions

To understand how to comply with these laws, we must first understand a couple of important definitions and how these definitions differ across the laws. Each of these laws broadly define the information protected thereunder. ColoPA, CT DPA, VA CDPA, and UCPA use the term "personal data," defined as information that is linked or reasonably linkable to an identified or identifiable individual. The CPRA uses the term "personal information," meaning information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California resident or household. All these laws exclude de-identified or publicly available data from these definitions. Further, ColoPA, CT DPA, VA CDPA, and UCPA do not regulate the personal data of individuals collected in the employment or business-to-business contexts, but California does. This means that, after January 1, 2023, the personal information that a business collects from its employees and its customer and/or vendor contacts who are California residents is now fully protected under the CPRA.

Each law varies slightly, but notably, in its definition of "sale" of personal data. The CPRA, ColoPA, and CT DPA define "sale" broadly as the transfer of personal data for monetary *or other valuable consideration*, while the VA CDPA and UCPA more narrowly define "sale" to require monetary consideration.

One of the most important aspects of these laws is the regulation of targeted advertising or cross-context behavioral advertising. The CPRA defines "sharing" as the transfer of personal information to a third party for "cross-context behavioral advertising," which is the targeting of advertising based on the individual's personal information obtained from activity across businesses, distinctly-branded websites, applications, or services. The ColoPA, CT DPA, VA CDPA, and UCPA utilize a similar definition for "targeted advertising," meaning displaying advertisements to a consumer based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests, subject to certain exceptions.

All of the new laws afford special treatment to "sensitive data" or "sensitive personal information," which include, among other things, information related to race or ethnicity, religion, health, sexual orientation, citizenship, and genetic or biometric data used to identify a person. Under the VA DCPA, ColoPA and CT DPA, a business must obtain consent from the individual prior to the processing such sensitive data. On the other hand, the CPRA and UCPA only require notice and an opportunity to opt out of or limit the processing of such data.

Compliance

Now, we can understand what compliance with these laws entails. Under each law, controllers (i.e., those that determine the purposes and means for processing personal data) must provide individuals with a reasonably accessible and clear privacy notice (i.e., privacy policy) that includes, among other

things, the categories of personal information collected or processed, the categories of personal information disclosed or shared with third parties, whether personal information is sold, the purposes for collecting or selling personal information, and the categories of third parties to whom information is disclosed or sold.

Additionally, under several of the new laws, businesses must perform a privacy impact assessment that weighs the benefits of processing for the controller against the potential risks for the individual *prior to* selling personal data, processing personal data for targeted advertising, or processing sensitive data. Each law also requires that all processors or service providers be subject to a written contract that expressly sets forth, among other things, the limitations on processing, the types of data being processed, the duration of processing, confidentiality obligations, audit rights for the business, deletion and return of personal data procedures, and subcontracting limitations.

Consumer Rights and Requests

The inclusion of certain rights for individuals regarding their own personal data is what sets these new privacy laws apart from previous privacy regulation in the United States. From a compliance perspective, these consumer rights, and how to facilitate them, are key considerations and could require substantial work for businesses. These consumer rights allow respective residents to: (1) access their personal data; (2) correct inaccuracies in their personal data (not provided in the UCPA); (3) delete their personal data; (4) obtain a copy of their personal data in a portable format; and/or (5) opt out of processing for purposes of the sale of personal data, targeted advertising, or profiling.

Businesses must provide one or more secure and reliable request methods, which are described in their privacy notice. Controllers must respond to requests within 45 days but have the ability to extend that period upon notice to the consumer. Under the ColoPA, CT DPA, and VA CDPA, businesses must go one step further and provide consumers a means to appeal a denied request.

Enforcement

So, what happens if you fail to comply? Most importantly, the ColoPA, CT DPA, UCPA, and VA CDPA do not create a private right of action for individuals. Rather, the states' Attorneys General are tasked with enforcement. Only in California do individuals have a private right of action, and it only applies to data breaches of non-encrypted and non-redacted personal information.

Additionally, the UCPA and VA CDPA provide a 30-day period for businesses to cure violations prior to the Attorney General seeking remedy, and, until January 1, 2025, the ColoPA and CT DPA provide 60-day cure periods. After January 1, 2025, the Connecticut Attorney General has discretion to offer a cure period, but the ColoPA does not expressly provide such discretion. The CPRA eliminates the cure period that was available under the CCPA, and so, after January 1, 2023, there will not be a mandatory cure period. Rather, the California Attorney General will have discretion to grant a cure period.

The types of penalties and fines that the Attorneys General may seek under these laws vary. The CPRA carries the possibility of fines up to $2,500 per violation or up to $7,500 for an intentional violation or a violation involving minors under age 16. CT DPA violations can result penalties up to $5,000 per violation, while the VA CDPA and UCPA each allow for fines up to $7,500 per violation. Lastly, a ColoPA violation can result in a fine up to $20,000 per violation, per consumer or transaction or up to $50,000 if committed against a person over 60 years old. As you can see, failures to comply with these laws can easily result in substantial fines.

Conclusion

Unless a federal law is enacted to preempt these state laws, the recent wave of state privacy legislation is not expected to slow down. Businesses should review the relevant laws and make plans for their compliance now. Consolidating your compliance efforts across all of these state privacy laws into one thorough compliance plan could save you and your business time and money now and from mistakes and fines later.