NOVEMBER 5, 2020

Legaltech® news

ONLINE

An ALM Publication

With the Passage of CPRA, California Privacy Law is Leaps and Bounds Closer to GDPR

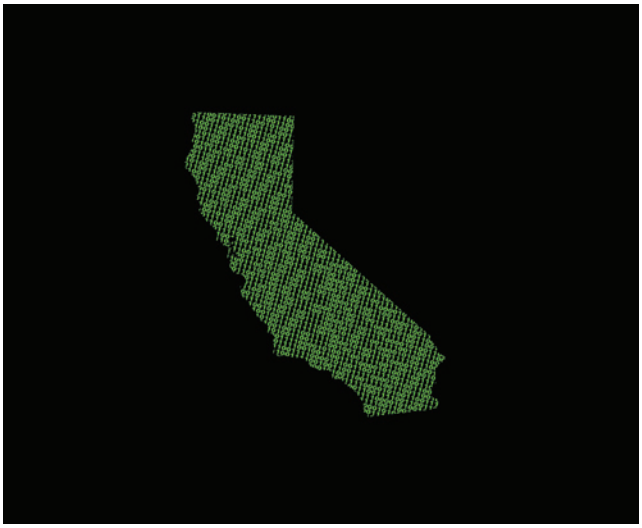
Any company currently obligated under CCPA will be affected by the passage of CPRA. And while many of the law's nuances are yet to be determined, there are a number of substantial changes that organizations need to understand, in order to prepare.

BY RYAN SMYTH, FTI CONSULTING

We made it. One of the most charged and anticipated elections in history, in one of the most challenging years our country has seen, is finally behind us. Regardless of what side of the aisle your votes were cast upon, we can all agree a lot was at stake in this year's elections, all the way down to the local level. One of the most notable initiatives among state ballots this year was the California Privacy Rights Act of 2020 (CPRA), which, as expected, passed with a majority vote.

In the simplest of terms, CPRA adds a lot of muscle to the existing stipulations in the California Consumer Privacy Act (CCPA). When CCPA was first enacted, it was widely compared to Europe's General Data Protection Regulation (GDPR), but in reality, the data privacy requirements in CCPA were only a small fraction of those in GDPR. That will ultimately change when CPRA takes effect in January 2023, and moves California privacy regulation closer to GDPR standards.

Over the next year or so, California lawmakers will begin creating the specific regulations and entities that will facilitate CPRA. The law will at that point become effective, and enforcement will begin in June 2023, with a lookback to January 2022. Any company currently obligated under CCPA will be affected by the passage of CPRA. And while many of the law's nuances are yet to be determined, there are a number of substantial changes that organizations need to understand, in order to prepare.



Key Changes Introduced with CPRA

CPRA is introducing numerous new requirements to strengthen California data privacy enforcement, as well as making modifications to CCPA. The most important provisions include:

- Solidifies current requirements in CCPA, to make it more difficult for legislators to soften CCPA in the future.
- Calls for the formation of a standalone data privacy authority (DPA) to enforce data privacy compliance, vs. the current model of oversight by the state attorney general. This new entity will be known as the California Privacy Protection Agency.
- Clarifies CCPA's current ambiguity around what constitutes the sale of data.
- Extends the CCPA's moratorium for employment and employee data from January 2021 to January 2023, which gives companies more time to operationalize for that condition.
- Adds email addresses and passwords to the list of protected data over which citizens may exercise private rights of action in the event of a data breach.
- Creates a subcategory of personal information(PI), which is similar to GDPR in defining higher-risk data as sensitive personal data (SPI). SPI will be afforded expanded data subject rights such as limiting the use and disclosure of this type of information.

• Requires any organization that is processing PI in a manner that presents significant risk to a consumer's privacy to conduct data protection impact assessments (DPIAs).

• Increases the penalties for failure to comply with stringent requirements for protecting the personal and sensitive data of minors.

• Allows data subjects to restrict or limit the use of their SPI, which will require organizations to add a "limit use of my sensitive personal information" opt-out function on their websites.

• Requires organizations that perform "cross context behavioral advertising" to provide a mechanism for individuals to opt out.

• Expands existing data subject rights in CCPA (right to access and right to delete) to include the right to correct information. Essentially, organizations will be required to take action on requests from data subjects to remedy incorrect or incomplete information.

• Introduces the GDPR concepts of data minimization and limitation—only keeping necessary data and only for as long as needed—as part of CCPA compliance.

• Requires organizations that use automated decision making and data subject profiling (which are often used in online ad targeting) to disclose those activities in their privacy notices.

Preparation Amid Uncertainty

This is a lot to take in, and as mentioned above, the finer details will be determined in the coming 24 months in the legislature. As many companies have already experienced with the enactment of GDPR and CCPA, the looming enforcement deadline often arrives faster than expected. It's important to get out in front of these changes as soon as possible, especially given that CPRA will include a lookback all the way to January 1, 2022. Moreover, the burden of responsibility—for educating consumers about the nuances between PI and SPI, or between sharing of data and selling data, protecting their data and enabling their data rights—falls upon the companies that process PI. Addressing each stage involved in this takes significant time and resources.

Focusing on the newly defined category of SPI is a good place to start. Similar to GDPR and CCPA, the key to understanding the landscape of SPI, and adhering to the laws for protecting it, is to maintain a robust data map. Existing data maps and methodologies may need to be adjusted to account for SPI. A detailed data map also significantly lightens the burden of responding to data subject requests and enabling limitations on how PI and SPI are used.

CPRA also introduces extensive rights for data subjects to limit what can be shared for the purposes of advertising. It allows data subjects to opt-out of onward transmission of their PI and sharing of their exact geolocation. These changes will bring significant implications for ad tech practices, as well as unique challenges for compliance and enforcement. Companies that process, sell, share or otherwise use this type of information as part of the advertising ecosystem need to watch the developments around this closely, and take steps to achieve transparency and compliance.

The significance of the CPRA's addition of data minimization and storage limitation also cannot be overlooked. Incorporating minimization and storage limitation (destruction) for PI into existing infrastructure and retention programs can easily become a multi-year effort. Organizations need to be prepared to document why retention of certain PI is necessary. Meeting these obligations will also involve getting a handle over the lifecycle of PI, defining what constitutes as end-of-life (i.e. when retention of the PI is no longer necessary to the business) and establishing controls for destroying PI accordingly.

Step-by-step, we're seeing a shift in the U.S. toward viewing and governing privacy much in the same way as Europe. CPRA should be considered as the likely blueprint other states will follow in the coming years. To truly prepare for a strong long-term privacy posture, organizations should look to CPRA and GDPR as guideposts against which to gauge their privacy frameworks. CPRA's effective date may seem like a long way off, but it—and likely other emerging state laws like it—will be here before we know it.

Ryan Smyth *is a Managing Director in FTI Consulting's Technology segment. He advises clients on a wide range of regulatory and compliance issues, with a specific focus on privacy, information security, data governance and business continuity. He brings deep business and technical background in the financial services industry, with more than 20 years of experience in governance, risk and compliance, data security and privacy programs. He has served in senior leadership positions at IBM, Promontory, and LPL Financial and held roles at UBS and Citigroup.*