STINSON

News & Insights

Privacy 2021 - Preparing for the CPRA

Alert

01.22.2021

By Steve Cosentino

If the past two years of ramping up compliance for the California Consumer Privacy Act (CCPA) wasn't fun enough, businesses have new compliance challenges ahead in the next couple of years. This past November, California voters passed the California Privacy Rights Act (CPRA). The CPRA was a ballot initiative that modifies and expands the CCPA. It adjusts the criteria for applicability, adds a category for sensitive personal information, gives individuals new rights and also expands some of the existing CPRA rights. It also creates a new private enforcement authority and adopts some principles from the GDPR. Businesses will need to start modifying their privacy practices ahead of the CPRA effective date, January 1, 2023.

Step one is simple; get the acronyms right. These two laws rival confusion between the now enjoined Children's Online Protection Act (COPA) and the alive and well Children's Online Privacy Protection Act (COPPA). After that, take a deep breath, as there is some time to comply. One positive is that the Business to Business and Employee exceptions have been extended from January 1, 2022 to January 1, 2023. Keep in mind, though, that the look-back period for privacy requests under CPRA will date back to January 1, 2022.

Another positive is on the applicability front. While the $25 million in annual revenue threshold remains, the threshold on buying, *sharing* or selling personal information was increased from 50,000 or more consumers, households or devices to 100,000 consumers or households. That increase in amount helps small businesses. The addition of the newly defined term "share" expands the scope of this threshold a bit. The definition of "sell" was broad to begin with, however, there is considerable overlap between these terms in the CCPA and CPRA. The main distinction is that "share" is limited to cross-context behavioral advertising and does not have a consideration element.

Privacy 2021 - Preparing for the CPRA

NEW CATEGORY FOR SENSITIVE DATA

One of the most visible and significant changes from the CCPA is the addition of a new "Sensitive Data" category. Prior to the CCPA, most U.S. government guidelines defining sensitive information were fairly general, focusing on information that could cause harm, embarrassment or unfairness. The CCPA definition is a little more specific, including government-issued identifiers such as social security numbers, financial account information, login credentials, geolocation information and information that exposes genetics, racial or ethnic origin, religious beliefs, biometrics, health data, sex life and sexual orientation. The CPRA does not require express consent like under the GDPR but it does give consumers more rights to limit the use and disclosure of sensitive information. As a practical matter, this could result in some more internal processing and procedures around data subject access requests (DSARs). Individuals could permit broader uses of their non-sensitive information while opting out of uses of their sensitive information.

PRIVATE RIGHT OF ACTION

The private right of action under the CCPA is one of the most concerning provisions for most businesses, given the likely proliferation of consumer litigation using that provision. Under the CCPA, the private right of action is focused on data breaches. The CPRA expands that right of action to include unauthorized access of email addresses and passwords or security questions. Businesses will want to increase their use of encryption for access credentials.

PROFILING

The CPRA adds some new provisions relating to profiling, which is a huge part of the ecommerce ecosystem. Profiling is the automated processing of personal information that is used to evaluate individual characteristics and preferences in order to predict behaviors, interests and actions. Given that the CPRA came from a ballot initiative advocated by consumer rights activists, the focus on profiling is not a surprise.

AUTOMATED DECISION-MAKING TECHNOLOGY

Using profiling across websites and platforms has long been a concern of privacy advocates. The CPRA requires that new regulations be promulgated to govern access and opt-out rights for automated decision-making technology, including transparency about the logic involved in such technology. While this component is a bit of a wait-and-see, businesses that derive significant value in the trade secret properties of their processing algorithms will want to take this into account. In order to be prepared for additional disclosures once the regulations go into effect, most businesses will want to begin to document more information about what their third party cookie and tracking technologies do.

Privacy 2021 - Preparing for the CPRA

SECURITY AUDITS

One particular component of the CPRA is not likely to have a major impact before 2023 but should be on the planning list. The new California Privacy Protection Agency along with the California Attorney General are charged with issuing new regulations to require annual risk assessments and audits, including an annual cybersecurity audit. Many businesses who process personal information but use vendors to host it rely on the security audits of their vendors for compliance purposes. This provision will likely mean that many businesses processing significant amounts of personal information will need to begin conducting internal privacy and security audits themselves, if they do not already do so.

INDIVIDUAL RIGHTS

The CPRA also adds some new individual rights. In addition to the new rights around Sensitive PI and Automated Decision Making, the CPRA grants a right to data correction. While this particular right is not likely to have a major effect on a business's use of personal information, it will require additional steps in the DSAR process and will be subject to further regulations.

DATA FROM CHILDREN

Businesses will want to be very careful when it comes to collecting and processing information from children. Fines under the CPRA are three times higher when a business has actual knowledge that the consumer is under 16. Also, with respect to children under the age of 16, the CPRA turns the statute into an opt-in law with respect to selling or sharing personal information. Businesses are prevented from repeatedly asking for consent for a year after the original request. Regulations will be adopted for an opt-out signal available to children and parents. Businesses who already comply with COPPA will be well on their way to complying with these new provisions of the CPRA but will need to take into account that the scope expands the definition of children to those under 16 as opposed to those under 13.

VENDOR DILIGENCE & DATA RETENTION

One of the most important compliance activities under the CCPA is to ensure that service providers enter into data protection addenda or other agreements to ensure that they are characterized as a service provider as opposed to a third party for CCPA purposes. Otherwise, sale opt-out rights apply which can hamper the ability, to provide basic services. The CPRA adds a new definition for contractors. Importantly, neither a contractor nor a service provider is a third party under the CPRA. However, a contractor is subject to additional requirements such as certification that it understands CPRA restrictions on use and disclosure and permission to monitor compliance with the contract. This addition may be helpful to many businesses in their vendor diligence programs.

There are some additional requirements on data retention requiring each business to inform consumers of the length of time the business intends to retain each category of personal and sensitive personal information, or if that isn't possible, the criteria used for such determinations. Businesses will want to review and update their document retention policies in the time leading up to January 2013.

EXEMPTIONS

Finally, one of the biggest issues for many businesses is the fate of the employee and B2B exemptions to the CCPA. As mentioned above, both of those are extended to January 1, 2023. We expect additional legislation to be put forth during that period to address those two critical exceptions. Unfortunately, it's another wait-and-see. Most CCPA privacy policy disclosures concerning these exemptions should be appropriate under the CPRA, although businesses should update them to change the end date to January 1, 2023 from January 1, 2022 if they have not already done so.

For more information on how to prepare for the CPRA, please contact David Axtell, Steve Cosentino or the Stinson LLP contact with whom you regularly work.

CONTACTS

David D. Axtell

Stephen J. Cosentino, CIPP

RELATED CAPABILITIES

Corporate Finance

Intellectual Property & Technology

Labor, Employment & Benefits

Private Business

Sports & Recreation