Insights: Alerts

CCPA 2.0: California Privacy Laws Continue to Take Center Stage

NOVEMBER 17, 2020

On November 3, 2020, California voters passed Proposition 24, the California Privacy Rights Act ("**CPRA**").

The provision's timeline is important to consider. The law would become effective on January 1, 2023 with enforcement set for July 1 of that year. Significant rulemaking under the law is required to be finalized by July 1, 2022, so the notice and comment process for those rules should begin next year.

Companies should develop compliance strategies accordingly, by developing high-level compliance strategies (e.g., scoping out exceptions to the CPRA to determine what portions of the law are in-scope). That analysis will prepare companies for finalizing compliance documents closer to the law's effective date (e.g., privacy rights requests web forms and privacy policies). We caution that regulations implementing the California Consumer Privacy Act ("CCPA") were not finalized by the statutory deadline. Businesses should therefore monitor rulemaking progress if waiting for regulatory guidance to finalize compliance documents.

What Should an Organization Start Doing Now?

As described in more detail in this alert, below is a list of the top steps to take in the coming months to prepare for CPRA compliance:

1. Review data maps or conduct data mapping to determine if the organization processes sensitive personal information and for what purposes. Begin developing a plan for making the personal information non-sensitive, such as through masking, or developing a process for allowing consumers to restrict the use of sensitive personal information.

2. If the organization has launched a "Do not Sell" button, then analyze whether the scope of that button allows consumers to opt out of newly defined "sharing". If the organization has not launched a "Do not Sell" button, determine if the organization "shares" personal information.

3. Identify retention periods for personal information collected from consumers, and decide whether those retention periods should be reconsidered before making the periods publicly available.

4. Outline a process for consumers to correct personal information, including to verify a consumer's claim that personal information is inaccurate.

5. If the organization acts as a service provider under the CCPA for all or part of its operations, evaluate whether new restrictions on service providers under the CPRA prohibit the organization from continuing to act as a service provider. Otherwise, update agreements with customers to include newly-required restrictions for

ensuring service provider status.

6. Explore enhancing email security practices, such as to require multifactor authentication and increase the frequency of mandatory password changes.

Moving Closer to the GDPR

Purpose Limitations on Businesses' Use of Personal Information. Familiar to those companies that prepared for the EU's GDPR, the CPRA creates a general purpose limitation on personal information use, limiting a business's use and sharing of personal information to the purposes for which it was collected and for other compatible purposes of which the consumer has been informed. The process for disclosing additional purposes may be the subject of rulemaking. Moreover, although the CCPA contains similar notice requirements with respect to the purposes for which personal information will be processed, the CPRA's expanded provisions may provide additional enforcement options for California regulators.

Retention Periods under Scrutiny, while Data Minimization Enters the Fold. As under the GDPR, businesses must publicly disclose the periods for which the business retains personal information. The CPRA requires businesses to disclose the length of time for which the business plans to retain the collected personal information in the business's notice to consumers at collection. Businesses must provide that period for each category of collected personal information. That section of the CPRA also develops a data minimization concept, by prohibiting businesses from retaining a consumer's personal information for longer than is necessary to achieve the disclosed purposes for which the information is collected.

New or Expanded Data Subject Rights

Another Link for Homepages. The CPRA, unlike the CCPA, defines “sensitive personal information,” and allows consumers to limit the purposes for which businesses may use sensitive personal information. Businesses must facilitate that right by providing a link on the business's homepage labeled "Limit the Use of My Sensitive Personal Information.” Geolocation information, one of the most commercially significant forms of sensitive personal information, is sensitive if it is accurate up to 1,850 feet (roughly equivalent to GPS coordinates containing two or fewer decimal places). Further, defining precise geolocation information is an area of mandatory regulatory guidance.

Illuminated Opt-outs: Right to Opt-out of Cross-Contextual Advertising. Although the CPRA creates a newly-defined consumer right to opt-out of sharing consumers' personal information, the CPRA's definition of “sharing” is quite limited and includes only disclosures for cross-context behavioral advertising. The “Do not Sell” my personal information button will therefore be replaced with a link labeled “Do not Share or Sell” my personal information.

The CPRA's newly-defined opt-out of sharing right may function to clarify, rather than to enlarge, the CCPA's opt-out of sale right. The CCPA defined “sale” broadly to include any disclosure for any monetary or non-monetary consideration. Many organizations reasonably determined that “sharing” personal information with a digital advertising counterparty was a “sale” under the CCPA as such disclosure provided mutual benefit. The CPRA's opt-out of sale does not necessarily expand consumer opt-out rights with respect to any business that made such a determination. The CPRA's “new” sharing opt-out instead works to resolve ambiguity regarding whether sharing for targeted advertising, that qualifies as cross-contextual, must be subject to an opt-out right even if the consideration

for such sharing is not obvious. That clarification will likely push some businesses that did not develop an opt-out for the CCPA to offer an opt-out right for such disclosures.

The CPRA defines cross-contextual advertising such that not all sharing for targeted advertising is subject to the new opt-out right. Cross-contextual advertising under the CPRA is targeted advertising based on a consumer's activity across multiple businesses, distinctly branded websites, applications or services. Cross-contextual advertising, however, does not include targeted advertising based on a consumer's interaction with "the business, distinctly-branded website, application, or service with which the consumer intentionally interacts." That list of contextual settings does not include "devices". Targeting advertisements based on a consumer's interaction with the same business in the same contextual setting (especially the same application or website, which are the narrowest categories of settings in the list) across multiple devices may not be cross-contextual under the CPRA. The opt-out of sharing may therefore not apply to disclosures necessary to facilitate such targeting (unless, of course, a business determines that such disclosures meet the CCPA's broad definition of sale).

A business determining that the business does share personal information may prefer to offer an opt-out of sharing rather than selling. Describing disclosures in the digital advertising system as "sharing" may more accurately reflect the disclosures. Such disclosures sometimes occur simply to facilitate advertising rather than to merely provide profit from a buyer with whom the "selling" business will have no future relationship. Given the meaning of "sell" to their customers, companies may have, when confronted with the term's ambiguous CCPA definition, hesitated to inform their consumer-customers that the business "sells" personal information.

New Right to Correct Personal Information. Under the CPRA, consumers may ask businesses to correct inaccurate personal information. The details of this right are uncertain as the operational processes for the right will be subject to agency rulemaking. Therefore, companies that have not already done so should develop a process for verifying the accuracy of consumers' claims that personal information is inaccurate.

Expanded Private Right of Action. The CPRA expands the CCPA's private right of action. The CPRA allows consumers to bring an action against businesses for the security breach of a consumer's email address in combination with a password or security questions and answers that allows for unauthorized access to a consumer's email account, in addition to the data elements included in the CCPA. This private right of action is available only if a business failed to implement reasonable security measures.

Contractual Requirements

New Restrictions on Service Providers. Both service providers and contractors (a new status under the CPRA that is functionally equivalent to a service provider) are prohibited from combining the personal information collected on behalf of one business with personal information collected independently or on behalf of another business.

Contractual Obligations on Buyers of Personal Information. The CPRA requires businesses that sell personal information to third parties to contractually require such third party buyers to, among other requirements, only use the purchased personal information for specified purposes and use the purchased personal information consistently with the CPRA.

New Obligations to Flow Down Deletion Requests. The CPRA expands obligations to pass on consumers' deletion requests. Businesses must notify all third parties to whom a consumer's personal information had been sold of a consumer's deletion request. However, that requirement does not apply if passing along such notice "proves

impossible or involves disproportionate effort". Buyers and sellers of personal information should update and clarify, through contract, each party's obligations to effectuate a deletion request that has been passed on to such party by the other party.

Expanded Government Oversight

New Mandatory Filing with a Government Agency. The CPRA enlists California's Attorney General to determine which businesses' personal information processing presents significant risks to the privacy or security of consumers' personal information. The Attorney General must require those businesses to submit a risk assessment to the newly-formed agency, the California Consumer Privacy Agency. Such businesses would also be required to complete an annual security assessment.

A New Enforcement Agency. As mentioned above, the CPRA creates the California Consumer Privacy Agency, which will assume enforcement and rulemaking authority from the Attorney General. Additionally, the CPRA provides the agency with the right to audit businesses' compliance with the CPRA and to investigate businesses following a consumer's complaint.

Related People



Jon Neiditz
t 404.815.6004
jneiditz@ktslaw.com