SAUL EWING ARNSTEIN & LEHR LLP

Alert

CYBERSECURITY AND PRIVACY PRACTICE

OCTOBER 2019

AUTHORS

APRIL F. DOSS

ALEXANDER R. BILUS

PATRICK M. HROMISIN

JILLIAN K. WALTON

CCPA Amendments and Draft Regulations Provide Some Clarity, Some Uncertainty, and Numerous Compliance Obligations

SUMMARY

Last year, the California legislature passed the sweeping California Consumer Privacy Act of 2018 (CCPA), a far-reaching privacy law that will impact business across the country. Now, in advance of the CCPA becoming effective on January 1, 2020, California's state lawmakers and Attorney General have weighed in with amendments and draft regulations to the CCPA that will substantially impact the steps businesses must take to become CCPA-compliant. This alert discusses: 1) a summary of the CCPA's scope and key provisions, 2) a timeline of key dates and next steps for the CCPA compliance; 3) a summary of the amendments; and 4) an overview of the draft regulations, so that companies can assess how they should proceed in light of these developments.

CCPA Summary and Scope

We have previously written about the CCPA here. The CCPA applies to for-profit entities that collect California residents' personal information, do business in California—even if they are not located in California—and:

- have annual gross revenue exceeding $25 million; OR
- sell or share for commercial purposes the personal information of 50,000 or more California residents, households, or devices; OR
- derive 50 percent or more of their annual revenue from selling the personal information of California residents.

The CCPA may apply to a nonprofit if the nonprofit controls or is controlled by a business that is subject to CCPA and shares common branding with that business.

The CCPA's rights and obligations center around a broad range of personal data, which the law defines as data that relates to individual consumers or households, and which specifically includes:

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- Characteristics of protected classifications under California or federal law;
- Commercial information, including online shopping and purchases;
- Biometric information;
- Internet activity;
- Location data;
- "Audio, electronic, visual, thermal, olfactory, or similar information";
- Education and employment information; and
- "Inferences" that are drawn from personal data to create a consumer profile "reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."

The CCPA also provides new rights to consumers, including:

- the **right to know** what personal information about them is collected, used, shared or sold,
- the **right to delete** personal information held by businesses,
- the **right to opt-out** of the sale of personal information, with more stringent opt-in and parental consent requirements for the sale of children under the age of 16 and 13, and
- the **right to non-discrimination** in terms of price or service when a consumer exercises a privacy right under CCPA.

And the CCPA imposes new obligations on businesses, including the obligations to:

- **Provide notice** to consumers before or at the time of data collection,
- **Create procedures** to respond to requests from consumers to opt-out, know, and delete information,
- **Respond** to requests from consumers to know, delete, and opt-out within specific timeframes,
- **Verify** the identity of consumers who make requests to know and to delete, and
- **Disclose** financial incentives for retention or sale of personal data.

Key Dates for CCPA Compliance

Although the legislature's amendments have been signed into law and thus are in their final form, the Attorney General's draft regulations are subject to a period of notice and comment before becoming final. As a result, there are still open questions as to what businesses' final obligations will be.

The key dates to note for CCPA compliance are the following:

- From December 2 through 5, 2019, the Attorney General will hold public hearings to solicit comments on the draft regulations in four cities throughout the state.
- December 6, 2019 is the deadline to submit written comments on the proposed regulations.
- On January 1, 2020, the CCPA, as amended, goes into effect.
- The draft regulations are expected to be finalized in the spring of 2020.
- Starting on July 1, 2020, the Attorney General's office will be empowered to enforce the provisions of the CCPA. In his press conference on October 10, the Attorney General indicated that his office will seek to penalize violations of the CCPA that occur between January 1, 2020 and July 1, 2020.
- On January 21, 2021, one-year exemptions relating to employee data and business-to-business data (discussed below) will expire. At that time, unless there are legislative developments within the next year, businesses will be required to fully comply with the CCPA for information collected from employees, job candidates, and between businesses.

Businesses that are subject to the CCPA therefore have to be prepared to comply with the law starting on January 1, but must also be ready to comply with the Attorney General's regulations when they become effective.

The Amendments to the CCPA

Despite intense lobbying efforts during the legislative session, the CCPA's core consumer protections and corresponding obligations on businesses remain relatively unchanged by California lawmakers. Below is a summary of the relevant amendments, which were passed as separate bills by the state Assembly.

One-year delay in effective date for certain employee, job applicant, and business-to-business information—but companies must still beware of breaches: Assembly Bills 25 and 1355 provide businesses with a one-year reprieve (until January 1, 2021) before they must implement CCPA compliance for employee and job applicant data, and for business-to-business communications and transactions. With respect to employee and job applicants, businesses still must inform individuals of the categories of personal information the businesses will collect from employees or job applicants and the purpose for which the information will be used. During this one-year moratorium, consumers, including job applicants and employees, will be able to sue, and employers may face liability to employees and/or job applicants as a result of a security breach of their non-encrypted or non-redacted personal information. With respect to business-to-business communications and transactions, during the one-year moratorium, businesses-to-business consumers have a private right of action for security breach incidents of non-encrypted or non-redacted personal information and the right to opt-out of the sale of personal information.

Slight narrowing of the definition of "personal information": Assembly Bill 874 narrows the definition of "personal information" somewhat by restricting it to information that is "reasonably capable of being associated with, or could reasonably be linked" to a particular consumer or household. This amendment also clarifies that personal information does not include de-identified or aggregate consumer information, and defines "publicly available information" to mean information that is lawfully made available from federal, state or local government records. That said, the definition of "personal information" remains very broad and applies to a wide swath of types of data.

Technical corrections: Assembly Bill 1355 provides a number of technical corrections to the CCPA. This amendment clarifies, among other things, that class action lawsuits may not be brought for data breaches when the compromised personal information is either encrypted or redacted (as originally passed, the CCPA had required both encryption and redaction), provides express authority for the Attorney General to establish rules and procedures on how to process and comply with verifiable consumer requests for specific pieces of personal information relating to a household, and clarifies the scope of the exemption for data that is covered by the Fair Credit Reporting Act.

Guidance on consumer requests: The amendments also provide guidance on the processes for consumer requests to exercise their CCPA rights. The CCPA originally required all businesses to provide two methods for consumers to submit access and deletions requests, including a toll-free telephone number. Assembly Bill 1564 modifies this requirement for businesses that operate exclusively online and have a direct relationship with consumers: these business are now only required to provide an email address for consumers to make requests to access and delete their data.

Data broker registry: Assembly Bill 1202 requires data brokers to register with the Attorney General, requires the Attorney General to make available a data broker registration on its website, and grants enforcement authority to the Attorney General to seek an injunction and civil penalties against any data broker who fails to register.

The Attorney General's Draft Regulations

The Attorney General's draft regulations, while still subject to public comment and potential amendment before becoming final, are notable because they change and expand businesses' obligations under the CCPA in several key ways. The draft regulations consist of seven articles that run 24 pages in length and relate to nearly every provision of the law. But as discussed below, the most critical draft regulations relate to the purpose of processing, responses to consumer requests, notices and reporting to consumers, and opt-outs.

Purpose Limitation

One of the most significant ways in which the draft regulations go beyond the text of the CCPA is in adding a purpose limitation requirement. Under the draft regulations, if a business intends to use a consumer's personal information for any purpose that was not disclosed to the consumer at the time the information was collected, the business must directly notify the consumer of this new use and must obtain explicit consent from the consumer for this new use. This requirement is relevant to many businesses that have found value in performing analyses on customer information they have already collected, whether for marketing, product development, or other purposes. Machine learning and enhanced data analysis have made these types of analyses common and valuable.

Under the draft regulations, though, if the purpose underlying the follow-on analysis of a consumer's information was not disclosed at the time the information was collected, the business will have to contact the consumer to both notify the consumer of this processing and obtain consent from the consumer. This requirement should lead businesses to analyze their privacy notices closely and take steps to align them with current and anticipated uses of consumers' personal information, because if the initial notice provided at the time of original collection of the data is sufficient, the secondary notification and consent will not be needed. To achieve this goal, the employees who are responsible for drafting privacy notices must coordinate with the operations and marketing personnel who typically derive value from follow-on analyses of consumer information.

Responses to and Verification of Consumer Requests

As discussed above, the CCPA creates a number of rights consumers can exercise with regard to their personal information. The draft regulations establish the procedures businesses must use when they receive requests from consumers to exercise their rights.

Since the CCPA was passed, businesses and commentators have been concerned about the possibility of individuals fraudulently making requests with regard to other people's personal information. So it is notable that the draft regulations provide guidance for businesses on what information to require in a request for purposes of verifying the identities of the consumer making requests. Once the initial request and verifying information have been submitted, businesses are generally to avoid requesting additional information for verification purposes. If, however, the business is unable to verify the requestor's identity, it may request additional information, but the additional information may only be used for verification, and must generally be deleted shortly after the business processes the consumer's request.

If, despite these steps, a business is unable to verify a requestor's identity, the draft regulations require the business to inform the consumer of the fact. Furthermore, if the request is for information disclosure, the business must explain the categories of personal information the business holds, without providing specific data relating to the particular individual who is the subject of the request. And if the request is for information deletion, the business is required to treat the request as a request to opt-out of the sale of that information.

The draft regulations also forbid businesses from disclosing certain types of information in response to CCPA requests: a business cannot disclose a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security questions and answers. And a business also now has discretion to decline to disclose specific personal information if the disclosure would create a "substantial, articulable, and unreasonable risk" to the security of the personal information, the consumer's account, or the business' own systems and networks. Neither the regulations nor the statute provide guidance as to what factors a business should use to determine the existence of such a risk, however.

The draft regulations also provide some guidance, and introduce some ambiguity, with regard to requests for deletion of personal information. They provide that in response to verified requests for deletion, businesses must de-identify the information, aggregate

the information, or permanently and completely erase the information from their existing systems "with the exception of archived or back-up systems." But they also state that, "[i]f a business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system is next accessed or used." Neither the CCPA nor the draft regulations provide any guidance with regard to determining when an archived or back-up system is "accessed or used," which raises the possibility that any movement of data over to a backup system could create a duty to erase data on that backup system. This is likely an issue that will be addressed during the comment period.

Reporting and Notices to Consumers

As discussed above, when businesses specify a purpose for their data collection in the notice they provide to consumers before or at the time of data collection, the draft regulations prohibit businesses from deviating from that stated purpose. The draft regulations also go farther than the statute by providing that businesses must specify the purpose of collection for each separate category of personal information they collect. They also establish requirements concerning the comprehensibility of consumer privacy notices, requiring businesses to draft them in a way that "provides consumers a meaningful understanding of the information being collected," uses "plain, straightforward language," "avoid[s] technical or legal jargon," and can be read on "smaller screens, if applicable."

The draft regulations also create a new reporting requirement for businesses that annually buy, receive for commercial purposes, sell, or share for commercial purposes the personal information of 4,000,000 or more consumers. These businesses must compile annual statistics on the number of requests they receive from consumers for access to their personal information, deletion of their personal information, or to opt-out of sales of personal information, as well as the business' response to those requests. Businesses must then disclose these statistics as part of their publicly available privacy policies or within a link included in their privacy policies.

Opt-Outs

One of the most significant, and potentially most unclear, new obligations in the draft regulations is a requirement to treat "user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism" as requests to opt-out of the sale of consumers' personal information. Neither the CCPA nor the draft regulations provide any guidance on questions, such as what mechanisms a business must use to detect relevant browser plugins or privacy settings, how to verify the identity the user of a browser, or whether to treat changes in consumers' browser settings as an abandonment of the opt-out. This issue is likely to be a topic of public comment, but businesses should begin considering how they will comply with a requirement like this if this draft regulation is implemented as it currently stands.

Additional Issues

In addition to the areas discussed above, the draft regulations touch on many aspects of the CCPA, including the treatment of personal information concerning minors, businesses' record-keeping obligations, information requests concerning households rather than individuals, and the classification of service providers.

Conclusion

As the above discussion should make clear, full CCPA compliance remains a moving target while the draft regulations remain open to comment and change. But businesses can take many steps until then to comply with the law's numerous requirements. We will continue to track developments on these issues as the comment period proceeds and the Attorney General issues final regulations.

Saul Ewing Arnstein & Lehr's lawyers are available to assist with any questions you may have regarding issues raised in this alert. For further information, please contact the authors of this alert, the Saul Ewing Arnstein & Lehr lawyer with whom you usually work, or any of the leaders of the firm's Cybersecurity and Privacy Group.

This alert was written by April F. Doss, chair of the Firm's Cybersecurity and Privacy Practice, Alexander R. Bilus, vice chair of the practice, Patrick M. Hromisin and Jillian K. Walton, associates in the practice. April can be reached at (410) 332-8798 or at April.Doss@saul.com. Alexander can be reached at(215) 972-7177 or at Alexander.Bilus@saul.com. Patrick can be reached at (215) 972-8396 or at Patrick.Hromisin@saul.com. Jillian can be reached at (412) 209-2537 or at Jillian.Walton@saul.com.

Did you find this information useful? Please provide your feedback here and also let us know if there are other legal topics of interest to you.