Lowenstein Sandler

Client Alert

Privacy & Cybersecurity

October 16, 2019

California Attorney General Releases Draft Regulations Under the California Consumer Privacy Act (CCPA): New Concepts, New Questions, and Few Clarifications

By The Privacy & Cybersecurity Team

What You Need To Know:

- **The Office of the Attorney General of California just issued new and far-reaching regulations under the CCPA that impose new obligations on businesses, service providers and other stakeholders.**
- **The Regulations require *all* businesses to compile and maintain records regarding compliance with certain aspects of the CCPA, with enhanced obligations on businesses that process data on 4,000,000-plus consumers.**
- **The Regulations specifically acknowledge that personal information is a business asset with monetary value, and recommends valuation methodologies for calculating its worth.**

After months of anticipation by the business and regulatory community, on Oct. 10, 2019, the California Office of the Attorney General (AG) issued proposed regulations (the Regulations) under the California Consumer Privacy Act (CCPA). The Regulations are open for public comment until Dec. 6, 2019, with a final version expected in the spring of 2020. While the Regulations include several clarifications of the CCPA, the AG also seeks to impose significant additional requirements on businesses, service providers and other stakeholders. Considering the ambitious nature of these Regulations and the range of industries impacted, the full implications may not be realized for some time.

Selected Highlights

- ***Notices of Collection.*** The Regulations detail key aspects of CCPA consumer notices and requests, including the following:
    - *Notice "at or before" Collection*. In line with the language in the CCPA, the Regulations require that Notice of Collection be provided "at or before" the collection occurs, but the Regulations clarify that the notice must "be visible or accessible where consumers will see it before any personal information is collected"; otherwise, the business may not collect any personal data from that consumer. The practical implication here is that simply including the Notice of Collection in a privacy policy posted on a business's website may not be enough to comply, and more affirmative, visible, just-in-time notification will need to be provided to consumers at every data collection point.
    - *Changing Purpose and Consent.* The Regulations provide that if a business seeks to use personal information for any purpose not stated in its initial Notice of Collection, it must first notify the consumer **and** obtain the consumer's explicit consent.
    - *Indirect Acquisition and Sale.* The Regulations impose notice requirements on businesses that do not collect

personal information directly from consumers but acquire it from other sources. If a business seeks to sell personal information obtained indirectly, it must either (1) notify the consumer directly regarding its plans to sell the information and the consumer's right to opt out of the sale, or (2) confirm with the source of the personal information that the Notice of Collection to the consumer was sufficient to cover the business's planned sale, **and** obtain a signed attestation from the source regarding the method used to deliver the Notice of Collection, and an example of the Notice of Collection.
    - *Opt-Out Notices.* The Regulations require businesses that do not presently sell personal information but **may** do so in the future to notify consumers regarding this potential sales activity. There is a lack of clarity regarding implementation of this requirement, but the ability of a business to quickly pivot in response to market shifts, business partner requests or other factors may be impaired.
    - *Honoring User-Enabled Privacy Controls*. The Regulations require businesses to treat user-enabled privacy controls, such as browser plugins or privacy settings, as valid requests to opt out from the sale of personal information. Among other consequences, businesses may no longer ignore "do not track" and will have to manage opt-outs at the consumer level (when possible), and at the device or browser level when a specific consumer is not identifiable.
    - *Accelerated Business Response*. The Regulations require businesses to implement Opt-Out Requests within 15 days of receipt. Requests to Know and Requests to Delete must be acknowledged within 10 days, and fulfilled within 45 days, of the date of receipt by the business, **not** the date the request was verified.
- ***New Notice of Financial Incentives.*** The Regulations require businesses to provide consumers with notice of any financial incentives (or price of service differences) that the business offers in exchange for the retention or sale of the consumer's personal information. Such notices must include the value of the consumer's data that forms the basis for offering the financial incentive.
- ***Valuation of Data.*** The Regulations require that financial incentives or price or service differentials be "reasonably related" to the value of the consumer's data. For this purpose, the Regulations explicitly acknowledge that personal information has a cognizable monetary value. Businesses may choose among seven approved methodologies for calculating the financial worth of personal information, or they may choose an alternative that is a "practical and reliable method of calculation used in good-faith."
- ***CCPA Applies to Online and Offline Activity.*** The Regulations provide express guidance on implementation of CCPA for businesses that operate online and offline, including the provision of Notices of Collection in brick-and-mortar environments. Businesses that only collect personal information offline and do not maintain websites also fall under the CCPA and are required to comply with the Regulations.
- ***Record-Keeping.*** The Regulations create new record-keeping and training obligations for all businesses, with enhanced requirements for businesses that annually buy, sell, receive or share for the business's commercial purposes personal information of 4,000,000 or more consumers.
- ***Minors.*** Businesses that collect personal information from individuals under 13 years of age are required by the Regulations to obtain affirmative authorization of sale of such information from the child's parent or guardian, in addition to any verifiable parental consent that may be required under the Children's Online Privacy Protection Act (COPPA). In order to sell personal information of consumers between the ages of 13 and 16, businesses must use a two-step opt-in process where the consumer must (1) clearly request to opt in and then (2) separately confirm his/her choice to opt in.
- ***Verification of Consumer Requests.*** The Regulations provide some guidance on methods for verifying the identity of consumers based on several factors including the sensitivity of the information requested.
- ***Categories of Sources for Data.*** The Regulations close a gap in the CCPA by clarifying that data may be sourced directly from consumers, and indirectly from other entities including the government and consumer data resellers.
- ***Privacy Policies.*** The Regulations provide guidance on the contents of consumer-directed privacy policies, which may be used as the repository of certain notices and information regarding requests. All covered entities and stakeholders should expect the need for lengthy, detailed privacy policies that must accurately reflect current practices and procedures.
- ***Service Providers.*** Unlike the CCPA, the Regulations require service providers to

respond to consumer requests within 10 days of receipt, even if only to advise the consumer to contact the business. The Regulations make it explicit that under the CCPA an entity may be a service provider for certain data but a business for other categories of data.

What's Next?

For those keeping track, the Governor of California just signed seven amendments to the CCPA. Covered businesses gain significant lead time to achieve CCPA compliance under AB 1355, which creates a one-year exemption from the CCPA for personal information acquired in the context of certain B2B communications or transactions, and AB 25, which confers a one-year moratorium on application of the CCPA to the personal information of job applicants, employees, business owners, directors, officers, medical staff and contractors that reside in California. The CCPA, as amended, becomes effective on Jan. 1, 2020, the final regulations are expected in the spring of 2020 (if not before), and the enforcement date is July 1, 2020. Whatever your industry or point of view on data privacy, the CCPA will become reality in less than three months.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

MARY J. HILDEBRAND CIPP/US/E
Partner
Founder and Chair, Privacy & Cybersecurity
T: 973.597.6308
mhildebrand@lowenstein.com

MATT SAVARE
Partner
T: 646.414.6911
msavare@lowenstein.com

EDGAR R. HIDALGO
Counsel
T: 973.422.6418
ehidalgo@lowenstein.com

MANALI JOGLEBAR CIPP/US/E
Counsel
T: 973.597.2540
mjoglekar@lowenstein.com

DIANE MOSS
Counsel
T: 973.597.2448 (NJ) / 212.262.6700 (NY)
dmoss@lowenstein.com

CARLY S. PENNER CIPP/US
Associate
T: 973.597.2516
cpenner@lowenstein.com