SQUIRE PATTON BOGGS

Proposed CCPA Regulations: Initial Overview and Highlights

October 14, 2019

On October 10, 2019, the California Attorney General (California AG) issued the long-awaited California Consumer Privacy Act (CCPA) Regulations (Proposed Regulations), along with an Initial Statement of Reasons (ISOR) explaining the Proposed Regulations. These Proposed Regulations not only fill in statutory gaps, but also create several substantive new requirements. Companies may submit comments through December 6, 2019, and several public hearings will be held in the first week of December. Our Data Privacy & Cybersecurity Practice can assist you in drafting comments to the California AG during this public comment period.

Although we are highlighting key points from our initial review of the Proposed Regulations and the ISOR, these materials are complex and will be subject to continued review by, and further guidance from, our team of experts. The final regulations that are adopted following the comment period may differ from the Proposed Regulations. As we will not have the final regulations until close to or after the effective date of January 1, 2020, **we are recommending that our clients take steps now toward developing consumer-facing documents, as well as internal policies and procedures, that reasonably comply with the Proposed Regulations pending the final outcome of the rulemaking process**.

What Is Addressed by the Proposed Regulations?

The Proposed Regulations focus on privacy notice mechanics and details; requirements for evaluating and responding to individual rights requests; and other miscellaneous issues. The Proposed Regulations do not, however, clarify exemptions, applicability thresholds or the meaning of "sale" under the CCPA. Notably, the California AG considered and rejected the concept of a "GDPR safe harbor" because the two laws have too many differences.

What Are the Biggest Changes?

Below, we outline the most notable provisions in the Proposed Regulations and the ISOR.

- **Deterrence of Fraud**: The Proposed Regulations specify how to authenticate a consumer's identity and other measures to prevent fraud by (i) implementing a verification system that takes into account data sensitivity; (ii) providing specific guidance for authenticating non-account holders (e.g., matching three data points and obtaining a signed declaration in order to release specific pieces of personal information [PI]); and (iii) issuing a blanket prohibition on disclosing the following sensitive data in response to a request:
  - 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
  - Security questions and answers
- **Notification at Point of Collection**: The CCPA requires most businesses to provide both a "notice at collection" and a more detailed website privacy notice. Key requirements regarding the "notice at collection" include:
  - At or before the point of collection, businesses must disclose the categories of PI collected, the business or commercial purpose for collecting the PI, notice of the right to opt-out of sale (if applicable) and a link to the more detailed privacy notice. For PI collected online, businesses can simply provide a link to the website privacy notice.
  - Businesses that do not collect PI directly from the consumer do not need to provide a "notice at collection." However, prior to selling any PI, such businesses must either (i) contact the consumer directly to provide notice of the right to opt-out, or (ii) obtain a signed attestation from the original source that such notice was provided.
- **Focus on Offline Interaction**: The Proposed Regulations require businesses to extend the same rights to offline activity, including providing offline notices and honoring rights requests via offline mechanisms in some cases.
- **Service Provider Clarifications**: The Proposed Regulations and the ISOR clarify the scope of the definition of "service provider" by confirming that it applies to entities providing services to nonprofits, government agencies and other entities that do not meet the definition of "business" and otherwise meet the conditions provided in the definition. In addition, the Proposed Regulations clarify that a service provider may not use PI from one business to provide services to another business or third party, except to detect data security incidents or protect against fraudulent or illegal activity.
- **Additional Requirements for Significant Processing Volumes**: A business that "alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers," must compile specified metrics regarding individual rights requests received and processed, and disclose this information within its privacy notice.
- **Opt-Out Button or Logo**: The Proposed Regulations do not provide the anticipated button/logo that can be used to opt-out of the sale of PI. A placeholder is included indicating the button/logo will be made available at a later time, at which point, the public will have the opportunity to provide comments.

- **Consumer Data Value Calculation**: The Proposed Regulations contain a method for calculating the value of consumer data. This method will need to be followed in order for a business to justify charging a different rate or providing a different quality of service in cases where consumers elect to opt-out of sale.
- **Procedural Details for Individual Rights Requests**:
  - **Opt-Out Requirements**: A consumer making a request to opt-out of the sale of PI does not need to be verified (unless the business has a good faith, reasonable and documented belief that the request is fraudulent). Businesses should act as soon as possible to effectuate an opt-out request, but no later than 15 days from receiving the request. Further, a business must convey the opt-out request to all third parties to which the business has sold the PI in the past 90 days (and confirm to the consumer when this is completed). If a consumer has user-enabled privacy controls on a browser or device that indicate a desire to opt-out of the sale, a business must honor these preferences as if they were a request to opt-out made directly by the consumer. Arguably, this could be interpreted to require businesses to honor Do Not Track signals.
  - **Responding to Rights Requests**: In the event a consumer submits a request to know or a request to delete outside of one of the designated avenues provided by the business, the business is required either to (i) handle it as though it were submitted properly, or (ii) reply to the consumer with details on how to properly submit a request. If a deletion request cannot be verified, the business must treat that consumer as having opted-out of the sale of their PI.
  - **Deletion Details**: The Proposed Regulations allow back-up and archival data to be deleted when it is next accessed. Businesses must also get two confirmations before deleting data in response to a request.
  - **Records Retention**: Certain information regarding consumer rights requests must be retained for a minimum of 24 months.
- **Additional Noteworthy Clarifications**:
  - **Authorized Agent**: The Proposed Regulations clarify the role of persons who are authorized to submit requests on a consumer's behalf and how a business should handle these interactions.
  - **Details on Treatment of Minors**: The Proposed Regulations provide greater details on how to handle the PI of minors under 16 and the applicable opt-in requirements before selling their data. The ISOR points to COPPA requirements and guidance for confirming that a parent or guardian has provided consent.
  - **Household Requests**: Details are provided on how to verify and handle household data in certain circumstances.

How We Can Help

Our Data Privacy & Cybersecurity Practice can help you determine whether, and to what extent, the CCPA and the newly issued Proposed Regulations will impact your business, as well as assist you in your overall CCPA compliance efforts. **We can also assist companies and industry groups in preparing comments for submission to the California AG during the public comment period**.

Contacts

Ann LaFrance
Co-Chair, Data Privacy & Cybersecurity Practice
Partner, New York
T +1 212 872 9830
E ann.lafrance@squirepb.com

Elliot R. Golding
Partner, Washington DC
T +1 202 457 6407
E elliot.golding@squirep.com

Lydia de la Torre
Of Counsel, Palo Alto
T +1 650 843 3227
E lydia.delatorre@squirepb.com

Glenn Brown
Of Counsel, Atlanta
T +1 678 272 3235
E glenn.brown@squirepb.com

Lauren Kitces
Associate, Washington DC
T+1 202 457 6427
E lauren.kitces@squirepb.com

India Scarver
Associate, Columbus
T +1 614 365 2719
E india.scarver@squirepb.com

Shalin Sood
Associate, Washington DC
T +1 202 457 6183
E shahlin.sood@squirepb.com