The Surprises In Proposed Calif. Consumer Privacy Regs

By **Gretchen Ramos and Kate Black** (October 18, 2019)

Gretchen Ramos

Kate Black

On Oct. 10, the California Attorney General's Office issued the California Consumer Privacy Act Proposed Regulations.[1] Stakeholders have until Dec. 6 to submit comments, and there will be four public hearings prior to that date.[2]

On the same day, the Attorney General's Office also published the Initial Statement of Reasons[3] describing the basis for each provision in the proposal. The ISOR includes a Standardized Regulatory Impact Assessment[4] because the economic impact of the CCPA is estimated to exceed $50 million annually once fully implemented. The California Department of Finance estimates the cost of CCPA compliance will range from $50,000 to over $2 million, depending on the size of the business and its data processing operations.[5]

Summary

As businesses prepare for the CCPA, effective Jan. 1, they should be particularly aware of the following new requirements contained in the proposals:

Privacy Policy Must Describe Verification Process

A business's privacy policy must describe (a) the verification process the business will use for consumer requests to know, delete and opt out, including the information consumers must provide for verification, and (b) how consumers can designate an authorized agent to make a request on their behalf.

Estimated Value of Consumer Data

Businesses offering financial incentives must provide consumers with an explanation of why the financial incentive is permitted under the CCPA, a good-faith estimate of the value of the consumer's data in relation to the financial incentive, and a description of the method used to calculate the value.

Two-Step Deletion Process

Businesses must have a two-step deletion procedure whereby a consumer submits a deletion request online and, thereafter, the business confirms the consumer wants their personal information deleted prior to honoring the deletion request.

Large Businesses Must Publish Rights Metrics

A business that annually buys, receives, sells or shares for commercial purposes the personal information of four million+ consumers must be able to disclose the number of requests to know, delete and opt out it received, the number it complied with, the number it denied and the median number of days to respond.

Partial Opt-Out Choices

A business can provide more granular opt-out choices for selling, including presenting a consumer with the opportunity to opt out of only certain types of sales or certain data categories for sale, as long as the business displays the global, full opt-out choice more prominently.

Notices to Consumers

Article 2 of the proposal contains notice requirements regarding three areas under the CCPA:

- Collecting consumer personal information;

- Selling consumer personal information (opt-out right); and

- Offering a financial incentive in exchange for the retention or sale of consumer personal information.

Privacy Policy[6]

The privacy policy must inform consumers of their right to know the personal information collected, disclosed, and sold; their right to deletion; their right to opt out of sales; their right not to be subject to discriminatory treatment by exercising their rights; whom to contact for more information; and the last date on which the privacy policy was updated. They also require that a business must include the following in its privacy policy:

- The process the business will use to verify the consumer, including any information the consumer must provide;

- Whether or not it sells personal information of minors under 16 years of age without affirmative authorization;

- How a consumer can designate an authorized agent to make a request on behalf of the consumer; and

- If the business annually buys, receives, sells or shares for commercial purposes the personal information of more than four million consumers, it must provide information about the number of requests to know, delete, and opt out, and the median number of days the business took to respond to such request.

Notice of Collection of Personal Information[7]

A business can meet the notice requirement by providing a link to the business's privacy policy. Where personal information is collected offline, a business can provide "notice on a printed form that collects personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to the web address where the notice can be found."

Notice of Right to Opt Out of Sale of Personal Information[8]

Notice of the right to opt out of sale should inform consumers of their right to direct a business that sells (or may in the future sell) their personal information to stop selling and refrain from doing so in the future. A business is exempt from providing a notice of the right to opt out if it does not and will not sell personal information during the time period during which the notice is posted, and it states this in its privacy policy.

The opt-out notice must also include information about:

- The web form and any offline method by which consumers can submit their opt-out requests online;

- Instructions on any other methods consumers can use to opt out; and

- The proof required when consumers uses an authorized agent to exercise their opt-out rights.

A business that sells personal information "shall post the notice of the right to opt-out on the internet webpage to which the consumer is directed after clicking on the'Do Not Sell My Personal Information'or 'Do Not Sell My Info' link on the website homepage or the download or landing page of the mobile application." A business that sells personal information will not be required to have the designated logo or button.

Notice of Financial Incentive[9]

Notice of financial incentives must include the following information regarding the incentive program:

- Summary of the financial incentive or price or service difference offered;

- Description of the material terms, including the categories of personal information implicated;

- How consumers can opt in;

- Consumers' right to withdraw; and

- Explanation of why the financial incentive is permitted under the CCPA,including a good-faith estimate of the value of the consumer's data at issue in relation to the financial incentive and a description of the method used to calculate the value.

Consumer Rights Requests

Business Practices for Handling Consumer Requests

Requests to Know and Requests to Delete Timing[10]

Businesses must meet the following timeline:

- Within 10 days of receiving a request, a business must confirm receipt and provide information about how it will process the request, including a description of the verification process, and when a consumer should expect a response;

- A business has 45 days to respond to a request, beginning when the request is received by the business; and

- A business can extend the response period to 90 days if it provides the consumer with an explanation of why the extension is necessary.

Any employee handling consumer rights requests must be trained on the CCPA.[11]

Submission Procedure to Delete[12]

The proposals call for a two-step deletion procedure whereby a consumer submits a deletion request online, and the business separately confirms the consumer wants their personal information deleted prior to honoring the deletion request.

Submission Methods for Requests to Opt Out of Sales[13]

Businesses are required to provide two or more methods for consumers to submit opt-out requests to prevent their data from being sold, including at least a web form and a clear link on the business's website. Given the Governor recently signed an amendment requiring e-commerce only businesses to have one request method.

The proposal allows businesses to provide more granular opt-out choices, including presenting a consumer with the opportunity to only opt out of certain types of sales or certain data categories for sale,as long as the business displays the global, full opt-out more prominently.

Special Rules Regarding Minors

Businesses who knowingly collect the personal information of children under the age of 13 must create and maintain a process for parental or guardian consent to the sale of personal information of the child. For children between the ages of 13-16, the business must identify a reasonable method for allowing the minor to opt in to data sales, and inform them of their right to opt out and the process for doing so.

Verification of Requests [14]

The proposals do not stipulate a particular method of consumer verification in conjunction with a rights request. Instead,businesses should implement risk-based approach for verification,weighing:

- The type, sensitivity, and value of the information;
- The risk of harm to a consumer posed by unauthorized access or disclosure; and
- The likelihood of fraudulent or malicious actors.

The proposals further permit businesses to outsource the authentication process using a third-party identification service.

Verification Via User Accounts[15]

If the consumer maintains a password-protected account with the business, the business may verify the customer through their account, so long as they require the consumer to re-authenticate before disclosing or deleting the consumer's data.

Verification Without a User Account[15]

The proposals specifically identify the standard of certainty businesses should use in their verification processes when there is no user account associated with the individual:

- Requests for the categories of personal information collected require the business to meet a reasonable degree of certainty, or the matching of at least two data points;

- Requests for the specific pieces of personal information require the business to meet a high degree of reasonable certainty, or the at least three matching data points; and

- Requests for deletion should be scaled according to sensitivity of the data, and the risk of harm posed. Low-risk deletion requests require a reasonable level of certainty, while sensitive data deletion requires a high degree of reasonable certainty.

Authorized Agents[17]

If an authorized agent submits a request on behalf of a consumer, a business may require the consumer to provide written authorization for the agent to act on their behalf, and verify their own identity with the business.

Where a business cannot verify the identity of the person making the request, it is not required to honor the request and must inform the person that it cannot verify their identity.

Responding to Requests

Requests to Know

Businesses must use reasonable security measures when transmitting personal information. A business:

- Is not required to provide specific pieces of personal information if such disclosure would create a "substantial, articulable, and unreasonable risk" to the security of the information, consumer account, or the business's security;

- Must never disclose a consumer's Social Security number, driver's license number, or other government-issued identification number; financial account number; health insurance or medical identification number; account password, or security questions or answers;

- Must inform consumers of the basis for its denial when it is based on a conflict with federal or state law or an exception to the CCPA; and

- Must provide an individualized response to a consumer request to know categories of personal information, sources and third parties and not refer to the privacy policy unless its response would be the same for all consumers.

Requests to Delete

A business can comply with a deletion request by either permanently erasing the personal information on its existing systems, de-identifying the personal information, or aggregating the personal information. The business must disclose the manner of deletion, and inform the consumer that it will keep a record of the deletion request. Where a business denies a deletion request it must inform the consumer of the basis for the denial,delete any information not subject to the exception, and not use the retained information for any other purpose that provided for by the exception.

Opt Out of Selling

In addition to the statutory requirements, if the information has already been sold to a third party, the business is required to notify the third party of the opt-out decision and instruct them not to further sell the data. Once completed, the business should notify the consumer that it has taken such action.

Documentation

Record-Keeping[18]

The proposals include new record-keeping requirements for businesses, including requiring businesses to:

- Keep a record of each consumer rights request received for at least 24 months;

- If the business receives, buys, sells, or shares the information of four million or more consumers,the business must keep, compile, and publicly post the following metrics regarding consumer rights requests:
    - The number of requests the business received for each right (know, delete, opt out);
    - The number of requests the business complied with and denied; and
    - The median number of days within which the business substantially responded.

Loyalty Programs, Nondiscrimination and Valuation of Data

Discriminatory Practices[19]

A business must notify consumers of any financial incentive price or service difference (i.e., a loyalty program) that it offers. The price difference must be reasonably related to the value of the consumer's data. A business cannot provide a different price or otherwise treat a consumer differently because the consumer exercised their right to know, opt out, or delete.

Calculating the Value of Consumer Data[20]

A business offering a loyalty program or financial incentive program, must use (and

document) a reasonable and good-faith method for calculating the value of their consumer data. The proposals identify various calculation methods, including "any other practical or reliable method".

Gretchen A. Ramos is a shareholder and co-chair of the data, privacy and cybersecurity practice, and Kate Black is a shareholder at Greenberg Traurig LLP.

[1] California Consumer Privacy Act Proposed Regulations, available at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf

[2] If the Attorney General's Office issues revised proposals, stakeholders will have fifteen days to file comments on the changes. Once finalized the AG's Office must transmit the final CCPA Regulations to the Office of Administrative Law (OAL) for review. OAL has 30 working days to conduct a review of the rulemaking record to ensure compliance with the OAL's regulations and the Administrative Procedure Act. Thus, the CCPA Regulations will not be finalized until after January 1, 2020, the effective date of the CCPA.

[3] Initial Statement of Reasons (ISOR), available at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf

[4] Standardized Regulatory Impact Assessment, available at http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf

[5] Initial Statement of Reasons (ISOR), Proposed Adoption of California Consumer Privacy Act Regulations (Stats. 2018, Ch. 55 [AB 375], as amended by Stats. 2018, Ch. 735 [SB 1121]), Ex. B, Department of Finance's Comments.

[6] § 999.308

[7] § 999.305

[8] § 999.306

[9] § 999.307

[10] § 999.313

[11] § 999.317

[12] § 999.312

[13] § 999.315

[14] § 999.323

[15] § 999.324

[16] § 999.325

[17] § 999.326

[18] § 999.317

[19] § 999.336

[20] § 999.337