GT GreenbergTraurig

Alert | Data, Privacy & Cybersecurity

February 2020

OAG Proposes Significant Changes to CCPA Regulations

On February 7, 2020, the California Attorney General's Office (OAG) issued proposed changes to the California Consumer Privacy Act Regulations (Modified Regulations), which were originally issued on October 11, 2019. Organizations have until February 24 to submit written comments on the proposed changes to the regulations implementing the CCPA.

Key Changes

Some of the major changes in the Modified Regulations include:

- **Accessibility Standard**. For notices and privacy policies provided online, businesses must follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium.
- **Opt-Out Button**. The Modified Regulations include an opt-out button that businesses can use on their websites to alert consumers of their right to opt out of sales of their personal information.
- **Service Provider Data Use**. The Modified Regulations clarify that service providers may use personal information internally to build or improve the quality of their services, so long as the use does not include building or modifying household or consumer profiles.

- **Valuation of Personal Information**. Under the Modified Regulations, if a business cannot calculate an estimate of the value of a consumer's data to show the rationale for its financial incentive program or price difference, the business cannot offer the financial incentive or price difference.
- **Recordkeeping**. In a supplemental update released February 10, the OAG increased from four million to 10 million the threshold number of consumers whose personal information a business must buy or sell for commercial purposes in order to be required to annually publicly disclose metrics of the numbers of consumer requests received, complied with in whole or in part, or denied.
- **Mobile**. The Modified Regulations are more explicit in their reference to mobile applications, including in relation to "Do Not Sell My Personal Info" opt-out links and just-in-time notices.
- **Personal Information Clarification**. Using IP address as an example, the Modified Regulations clarify that some reasonable linkage, whether direct or indirect, to a particular consumer or household is necessary in order for information to be characterized as "personal information" (PI).

The below provides a more detailed overview of the changes found in the Modified Regulations.

Definitions

The Modified Regulations add definitions for the terms "COPPA," "Employment benefits," "Employment-related information," "Signed," and "Value of consumer's data," and revise the definitions for "Categories of sources," "Categories of third parties," and "Household."

- "Categories of sources" is revised to require that the type or groups of persons or entity from which a business collects personal information about the consumers must be "**described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity**." The definition is also revised to note that the sources can include "the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers."
- "Categories of third parties" is also revised to include the same "described with enough particularity" requirement as the "Categories of sources" definition.

Guidance Regarding the Interpretation of CCPA Definitions (§ 999.302). The Modified Regulations added this new section presumably to explain the limitations to the CCPA's broad "personal information" definition. Section 302 reiterates the CCPA's "personal information" general definition, and then notes that if a website owner "collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, **then the IP address would not be personal information**." The level of abstraction with which such a reasonable linkage will be interpreted remains an open question.

Notices to Consumers

Overview of Required Information (§ 999.304). The Modified Regulations add an "Overview of Required Notices" section, instructing in-scope businesses that they must provide a privacy policy, a notice at the time of collection, a notice of the right to opt out if they sell personal information, and a notice of any financial incentives or price or service differences. Overall, however, the Article 2 "Notices to Consumers" section has few significant changes.

Notice at Collection of Personal Information (§ 999.305). The Notice at Collection section includes the following language relating to accessibility standards, mobile applications, and telephone collection:

- Accessibility. For notices provided online, businesses must follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In fact, this accessibility language is also included in § 999.306-.308, addressing other notices, including the right to opt out, notice of financial incentive, and privacy policy accessibility. Incorporating the WCAG v2.1 technical standards in different portions of an online digital property may represent a potentially unforeseen technical investment for some businesses.
- Mobile Application.
  - When a business collects personal information through a mobile application, it may provide a link to the notice on the mobile app's download page and within the application, such as through the application's settings menu. A mobile app may include a link to the privacy policy in the application settings menu as well.
  - When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, the business shall provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection.
- Telephone. When a business collects personal information over the telephone or in person, it may provide the notice orally.

Notice of Right to Opt Out of Sale of Personal Information (§ 999.306). In relation to the Notice of the Opt-Out Right, the Modified Regulations propose a new opt-out button to be used. When the opt-out button is used, it is to appear to the left of the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link and must be approximately the same size as other buttons on the business's webpage.

The Modified Regulations also add language that a business shall not sell the personal information it collected during the time the business did not have a right to opt out notice posted, unless it obtains the affirmative authorization of the consumer.

Responding to Requests to Opt Out (§ 999.315). The Modified Regulations do include two new requirements for businesses:

- A business's opt-out method should only require minimal steps, and cannot include methods designed to subvert or impair a consumer's decision to opt out.
- A business cannot use pre-selected settings for a consumer's right to opt out. Instead, the consumer must be allowed to make an affirmative selection.

Notice of Financial Incentive (§ 999.307). The Modified Regulations add language requiring a business to explain to the consumer **the material terms** of a financial incentive or privacy or services difference; that such notice be available where consumers will encounter it before opting in to the financial incentive; and the notice must now also describe the value of the consumer's data along with an explanation of **how the financial incentive is reasonably related to the value of the consumer's data**.

Consumer Rights Requests

Practices for Handling Consumer Requests

Submission Methods for Right to Know and Right to Delete (§ 999.312). The Modified Regulations' process for submitting requests to know and requests to delete remain largely intact.

Still, there are three noteworthy changes to this section:

- The Modified Regulations clarify that a business operating exclusively online shall only be required to provide an email address for submitting rights requests – although such a business must still provide two designated methods for deletion requests.
- The Modified Regulations require in-person businesses (such as stores or restaurants) to consider providing an in-person method for requests to know and requests to delete, including a printed form or a tablet or phone.
- The Modified Regulations no longer require a business to use a two-step process for online requests to delete. Instead, the business may implement a two-step process to confirm deletion requests.

Responding to Requests to Know and Requests to Delete (§ 999.313). The Modified Regulations do not substantively change the timeline for a business's response. Businesses must still provide confirmation of receipt within 10 days and respond to the request within 45 calendar days (unless an extension is required, in which case the business may extend the response period an additional 45 calendar days).

Denying a Request to Know. The Modified Regulations remove the risk-based approach for denying a consumer's right to know, wherein a business could deny a request to know if the disclosure creates a substantial security risk. The Modified Regulations instead create a clearer standard, in which a business is *not* required to produce personal information in response to a request if all of the below conditions are met:

- The business does not maintain the personal information in a searchable or reasonably accessible format;
- The business maintains the personal information solely for legal or compliance purposes;
- The business does not sell the personal information and does not use it for any commercial purpose; and
- The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.

Responding to a Request to Know Categories. The Modified Regulations add new disclosures a business must make in response to a request to know categorical data. In addition to the categories of personal information sold and personal information disclosed for a business purpose, a business must also provide the consumer the categories of third parties to which the business provided that particular category of personal information.

Denying a Request to Delete. The Modified Regulations requirements for responding to deletion requests remain largely intact. However, the Modified Regulations include a refined requirement for businesses that cannot verify an individual making a deletion request: the business must ask the unverified consumer if they would instead like to opt out of the sale of their personal information.

Service Providers (§ 999.314). The Modified Regulations add specificity to the process a service provider should follow if they receive a request to know or a request to delete. Under the Modified Regulations, a service provider shall either **act on behalf of the business, or inform the consumer that the request cannot be acted upon** because the request was sent to a service provider. The Modified Regulations remove the requirement that a service provider provide the consumer with the contact information of the appropriate business.

Requests to Access or Delete Household Records (§ 999.318). The Modified Regulations include additional, specific steps a business must follow before granting a request for access or a request for deletion regarding household information. The business must meet the following three requirements:

- The business must confirm all consumers of the household are jointly requesting access to specific pieces of information for the household or the deletion of household personal information,
- The business must individually verify all members of the household, and
- The business must verify that each member making the request is currently a member of the household.

Consumer Request Records Keeping (§ 999.317). The Modified Regulations make only slight modifications to the consumer requests records requirements:

- The business must implement reasonable security for the records, and
- The business shall not share these records with any third party.

On February 10, 2020, the OAG significantly clarified that instead of four million being the threshold for determining whether a business must compile public metrics from the previous calendar year regarding the numbers and dispositions of consumer requests received, now this requirement applies to: "A business that alone or in combination buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of **10,000,000** or more consumers in a calendar year."

Verification of Consumer Requests

The Modified Regulations leave the verification process largely unchanged, but do include three updates.

First, Section 323 of the Modified Regulations clarify that a business may not charge a consumer for verifying their request. For example, the business may not require an individual to submit a notarized affidavit unless the business compensates the consumer for the cost of the notarization.

The Modified Regulations also provide updated verification examples, utilizing less sensitive personal information for verification purposes. For example, where the original draft regulations previously advised businesses to use credit card security codes as an aid to verification, the Modified Regulations now include recently purchased items instead.

Finally, the Modified Regulations require businesses that believe they are unable to provide a reasonable method of verification to the degree of certainty required to include such a rationale in the business's privacy policy.

Authorized Agents (§ 999.326). The Modified Regulations include two new requirements **for authorized agents**:

- They must implement reasonable security to protect the consumer's information, and
- They may not use the consumer's information for any purpose other than to fulfill the consumer's requests, for verification, or for fraud prevention.

Clarified Standards for Service Provider Data Use

The Modified Regulations identify how a service provider is permitted to process personal information. The service provider may not retain, use, or disclose personal information obtained in the course of providing services, except to:

- **perform the services** specified in the written contract with the business that provided the personal information;
- **retain and employ a subcontractor**, where the subcontractor meets the requirements for a service provider under the CCPA and the regulations;
- **build or improve the quality of its services internally**, *provided that the use does not include building or modifying household or consumer profiles*, or cleaning or augmenting data acquired from another source;
- **detect data security incidents**, or protect against fraudulent or illegal activity;
- **comply** with federal, state, or local laws;
- comply with **civil, criminal, or regulatory inquiries** and investigations;
- cooperate **with law enforcement agencies**; or
- exercise or defend **legal claims**.

The specific exclusion in Section 999.314(c) for service providers not being allowed to retain personal information for "building or modifying household or consumer profiles" is likely very relevant for data-driven marketing participants.

Loyalty Programs, Non-Discrimination & Valuation of Data

Discriminatory Practices (§ 999.336). The Modified Regulations include significant updates to the requirements regarding discriminatory practices. Under the Modified Regulations, if a business cannot calculate an estimate of the value of a consumer's data to show the rationale for its financial incentive program or price difference, **the business cannot offer the financial incentive or price difference**.

The Modified Regulations also provide significantly updated illustrative examples for when a rights request denial may be considered discriminatory:

- A clothing business offers a loyalty program whereby customers receive a $5-off coupon to their email address after spending $100 with the business. A consumer submits a request to delete all personal information the business has collected about them but also informs the business that they want to continue to participate in the loyalty program. The business may deny their request to delete as to their email address and the amount the consumer has spent with the business because that information is

necessary for the business to provide the loyalty program requested by the consumer and is reasonably anticipated within the context of the business's ongoing relationship with them.

- A grocery store offers a loyalty program whereby consumers receive coupons and special discounts when they provide their phone numbers. A consumer submits a request to opt out of the sale of their personal information. The retailer complies with their request but no longer allows the consumer to participate in the loyalty program. This practice is discriminatory unless the grocery store can demonstrate that the value of the coupons and special discounts are reasonably related to the value of the consumer's data to the business.
- An online bookseller collects information about consumers, including their email addresses. It offers discounts to consumers through browser pop-up windows while the consumer uses the bookseller's website. A consumer submits a request to delete all personal information the bookseller has collected about them, including their email address and browsing and purchasing history. The bookseller complies with the request but stops providing the periodic coupons to the consumer. The bookseller's failure to provide coupons is discriminatory unless the value of the coupons is reasonably related to the value provided to the business by the consumer's data. The bookseller may not deny the consumer's request to delete as to the email address because the email address is not necessary to provide the coupons or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

***

Contact the Greenberg Traurig Data, Privacy & Cybersecurity team to discuss your organization's privacy program, data governance, and information security-related needs. Follow the GT Data Privacy Dish blog for more information on the latest privacy developments and insights.

Authors

This GT Alert was prepared by **Kate Black and Gretchen A. Ramos**. Questions about this information can be directed to:

- Kate Black | +1 305.579.0500 | blackk@gtlaw.com
- Gretchen A. Ramos | +1 415.655.1319 | ramosg@gtlaw.com
- Or your Greenberg Traurig attorney

also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2020 Greenberg Traurig, LLP. All rights reserved.