CLIENT ALERT

Proposed CCPA Regulations from California Attorney General: Part III – An Analysis of the Requirement to Verify Consumer Requests and Parental Consents

Nov.13.2019

On October 10, 2019, California Attorney General Xavier Becerra announced a long-awaited notice of proposed rulemaking and draft regulations for the California Consumer Privacy Act (CCPA), California's new consumer privacy law, which we have analyzed here and here.

In parts one and two of our multi-part series regarding the draft CCPA regulations, we focused on businesses' notice obligations and handling consumer requests.

In this third part of our series, we focus on proposed regulations regarding "verifiable" consumer requests, including the standards for verifying different types of requests received from consumers. As discussed below, the proposed CCPA regulations provide detailed guidance that will have important ramifications for businesses that possess or process consumer information.

Before the CCPA regulations are approved and implemented, interested parties have until December 6, 2019, to submit written comments regarding the draft regulations and to participate in town hall meetings hosted by the Attorney General's Office in Sacramento, San Francisco, Los Angeles, and Fresno.

Representatives of the Attorney General's office have indicated that July 1, 2020 is the anticipated date for CCPA enforcement to begin, but reiterated that CCPA takes effect on January 1, 2020.

"Verifiable" Consumer Requests Under CCPA

Verifiable consumer requests are a key concept under the CCPA. Most affirmative obligations for businesses are triggered only on receipt of a "verifiable" request—including the duty to respond to "requests to know" and "requests to delete" personal information. Cal. Civ. Code §§ 798.100-115. Businesses are not required to honor these requests, however, if the business cannot confirm the requesting party is the consumer whose information is sought or a person authorized to act on that consumer's behalf. Proposed Regulations § 999.313(c)-(d).

The CCPA offers little guidance on what makes a request "verifiable." Cal. Civ. Code § 1798.130(a)(2). Instead, this is detailed in the proposed regulations. Cal. Civ. Code §1798.140(y).

Here, we address Article 4 of the proposed regulation, which sets forth a process for determining whether a consumer request is "verifiable" and what that means for businesses.

ARTICLE 4: REGULATORY REQUIREMENTS FOR VERIFIABILITY

All businesses must "establish, document, and comply with a reasonable method" of verification that takes into consideration the type, sensitivity, and value of the personal information at issue and the risk of harm to the consumer posed by any unauthorized access or deletion. Proposed Regulations §999.323. This can be done either through a third-party service, or by matching data provided by the consumer to data already held by the business. The relationship between consumer and business prior to the submission of a consumer request is critical to verifying a request.

For **consumers with an existing password-protected account** with a business, businesses can use the existing password authentication process "if they implement reasonable security measures to detect fraud." Proposed Regulations § 999.324. However, businesses that suspect fraudulent or malicious activity on a password protected account must undertake "further verification procedures" before complying with requests to know or to delete received from that account.

For **non-account holders**, or those who "**cannot access**" a password-protected account, there are different verification standards based on the level of risk of the request. Proposed Regulations § 999.325.

- **Requests for disclosure of categories of personal information** must be verified to a **"reasonable degree of certainty.**" "A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business, which the business has determined to be reliable for the purpose of verifying the consumer." Proposed Regulations § 999.325(b).
- **Requests for disclosure of specific pieces of personal information** must be verified to a "**reasonably high degree of certainty**," which is a higher bar for verification. "A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request." Proposed Regulations § 999.325(c).
- **Requests to delete** may require verification to "**a reasonable degree or a reasonably high degree of certainty** depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion." "For example, the deletion of family photographs and documents may require a reasonably high degree of certainty, while the deletion of browsing history may require a reasonable degree of certainty." Proposed Regulations § 999.325(d).

Reasonableness is necessarily a fact-specific inquiry that businesses will have to undertake.

In addition, businesses may need separate processes to handle requests for disclosure of "specific pieces of information" versus "categories of information" collected.

Notably, the proposed regulations provide examples and not requirements for the information-matching standards for "reasonable certainty" and "reasonably high certainty." This distinction will be valuable for businesses that do not store information in a format easy to match to consumer inquiries, or may store only sensitive information and do not want to require consumers to transmit sensitive information in order to facilitate matching. Businesses that cannot meet the requisite degree of

certainty must refrain from complying with the unverified request and inform the requesting consumer of the reason for denying the request, and give a reason for the lack of ability to identify the requestor. Proposed Regulations § 999.325(f).

Article 4 also provides guidance regarding submission of a request to know or a request to delete by an authorized agent of the consumer. Proposed Regulations § 999.326. When a consumer uses an authorized agent to submit a request, the business may require that the consumer: (1) provide the authorized agent written permission to do so; and (2) verify their own identity directly with the business. A business may deny a request from an agent that does not submit proof that they have been authorized by the consumer to act on their behalf.

Verifying Parents & Special Rules for Minors

The CCPA includes special restrictions on the sale of children's personal information. Businesses must obtain different special "opt-in" consents for the sale of personal information if they wish to sell information of minors under 13, or information of minors 13 to 16 years of age.

For minors under 13, businesses must obtain affirmative consent to the sale of the child's personal information from the child's parent or guardian and reasonably ensure that the person providing the consent to the sale is the child's parent. The proposed regulations give a number of example methods a business could use that would satisfy this obligation, including:

- Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;
- Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;
- Having a parent or guardian call a toll-free telephone number staffed by trained personnel;
- Having a parent or guardian connect to trained personnel via video-conference;
- Having a parent or guardian communicate in person with trained personnel; and
- Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information, where the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete. Proposed Regulations § 999.330(a)(2).

The CCPA and its associated regulations specifically indicate that these restrictions on the sale of minors' personal information are *in addition* to any that might be imposed by the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. sections 6501, et seq.

For minors 13 to 16 years of age, businesses must allow the minors themselves to "opt-in" to the sale of their information. This process mirrors the "opt-in" process available to consumers who have previously exercised their "opt-out" rights – authorization must be obtained via two-steps through which the minor consumer "shall, first, clearly request to opt-in and then second, separately confirm their choice to opt-in." Proposed Regulations § 999.331.

Overall, the draft regulations offer substantial information on how to comply with CCPA obligations, and offer stakeholders an opportunity to weigh in on the final rules. The Attorney General's office will accept comments through December 6, 2019.

We will soon be posting additional analysis of the special obligations of service providers under Article 3 of the proposed regulations, as well as guidance on financial incentives.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Kristin J. Madigan, CIPP/US
Partner – San Francisco
Phone: +1 415.365.7233
Email: kmadigan@crowell.com

Paul M. Rosen
Partner – Los Angeles, Washington, D.C.
Phone: +1 213.443.5577, +1 202.624.2500
Email: prosen@crowell.com

Jeane A. Thomas, CIPP/E
Partner – Washington, D.C., Brussels
Phone: +1 202.624.2877, +32.2.282.4082
Email: jthomas@crowell.com

Lee Matheson, CIPP/US/E/A, CIPM, PCIP
Associate – Washington, D.C.
Phone: +1 202.654.6728
Email: lmatheson@crowell.com