Published on *The National Law Review* https://www.natlawreview.com

# CCPA Proposed Rules: Trust Less, Verify More

Article By:

Tara N. Cho

On October 10th California Attorney General Becerra released a set of proposed regulations as required by the California Consumer Privacy Act, which we have posted about here, here, and here. Although the draft rules do not incorporate the amendments passed by the legislature because they were not signed by the Governor until October 12th, the AG's proposals offer plenty to digest, debate, and comment upon.

Apart from whether one concludes that the proposed rules clarify or confuse what is expected under the CCPA, two topics in particular require organizations to rethink current practices. First, the CCPA requires an organization to respond to verified consumer requests concerning a person's information without saying much about what verification is required. Second, the law directs businesses that do not collect personal information directly from the consumer to undertake significantly more diligence about how the providing company has acquired the personal information. One thing about these two requirements is clear from the proposed regulations: it brings "trust but verify" to a whole new level.

## Verifying Consumer Requests

Three provisions within the CCPA (Cal. Civ. Code §§ 1798.100, 1798.110, and 1798.115) detail a consumer's right to know certain details about what personal information a business holds about them, where the information was obtained, and where the business has disclosed or sold the information. Section 1798.105 provides that a consumer may request that their personal information be deleted, subject to certain exceptions. Both the request to know and the request to delete are triggered by a verified consumer request, begging the question of what level of verification is appropriate.

It makes sense that one would want to confirm the identity of such a request, lest a business seeking to comply with a "request to know" inadvertently has a data breach by disclosing the personal information details to the wrong party. (Annie Bai of Socure and I wrote a piece in August for IAPP on the risks.) Unsurprisingly, the proposed regulations instruct a business to establish, document, and comply with a "reasonable" method for verifying that the person making the request is indeed the consumer to whom the information relates.

The AG has proposed that the following factors contribute to determining a "reasonable" verification approach:

1798. The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive or valuable personal information shall warrant a more stringent verification process. The types of personal information identified in Cal. Civ. Code § 1798.81.5(d) shall be considered presumptively sensitive;

1799. The risk of harm to the consumer posed by any unauthorized access or deletion. A greater risk of harm to the consumer by unauthorized access or deletion shall warrant a more stringent verification process;

1800. The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be;

1801. Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated;

1802. The manner in which the business interacts with the consumer; and

1803. Available technology for verification.

You got that? Is it clear now what will be considered a 'reasonable method'? The answer is that you do not, and the unfortunate reason is that not one of these factors help a business to identify a person as whom they claim. Identity management is difficult and the studies that Annie Bai and I discussed in our IAPP article provide evidence of how easily it is to spoof identity.

The CCPA and the proposed rules are right to want a business not to simply trust a requester but to instead insist upon some level of proof, but they seek this with little more than suggestions like 'require more rigorous proof for more sensitive data,' which is almost insulting.

## Obtaining Personal Information from another party

The proposed rules are acknowledged by the AG's team as adopting certain aspects of the EU's General Data Protection Regulation (GDPR), and one example of this appears in the context of obtaining personal information from a source other than the consumer. The GDPR directs that if an organization has collected information from a third party then typically the organization must promptly inform the individual that the organization now holds information about the person, what the applicable privacy policies are, and that the person has certain rights about how their information will be used.

The proposed CCPA regulations similarly direct that if a business has received a consumer's information and anticipates selling that information, the business must inform the consumer about their right to opt out from such sales. Interestingly, the proposed rules provide an alternative to informing the consumer that their information has been collected by a new business.

If the business wants to avoid contacting the consumer, it can turn to the source of the information and obtain assurances that the personal information was originally collected and shared with the new business in compliance with the CCPA. But really, where has the trust gone? It is no longer sufficient for the data source to provide a rep that they comply with applicable laws including the CCPA. While that is required, the proposed rules specify that the receiving business:

999. Confirm that the source provided notice to the consumer at the time of collection in accordance with Article 2 § 999.305, subsections (a) and (b) of the proposed regulations; and

1000. Obtain signed attestations from the source describing how the source gave the notice at collection and including an example of the notice. Attestations shall be retained by the business for at least two years and made available to the consumer upon request.

It remains understandable that the business receiving the information may not want to provide its own notice and opt out to the consumer, but that may be unavoidable for some time given the likelihood that little if any consumer information currently available for purchase has been subject to CCPA-compliant notices along with any level of diligent documentation of how the notice was provided.

The proposed rules are open to comment until December 6th.



National Law Review, Volumess IX, Number 291