INSIGHT: Decoding CCPA's Final Regulations Before Act Takes Effect

Akin Gump
STRAUSS HAUER & FELD LLP

Originally published in Bloomberg Law, June 29, 2020

Akin Gump attorneys examine the California attorney general's proposed regulations for the state's sweeping privacy law and outline what businesses subject to the law must consider to ensure compliance as they prepare to implement the regulations.

On June 1, the California Attorney General's Office (AGO) submitted its long-awaited final proposed regulations under the California Consumer Privacy Act to the California Office of Administrative Law (OAL).

Cognizant the enforcement date under the CCPA statute is set for July 1, the attorney general requested an expedited 30-day review and approval by the OAL. Once approved, the final text of the regulations will be filed with the secretary of state and become enforceable by law.

The regulations remain generally unchanged from the prior version posted on March 11, but the accompanying documents provide some additional insight in the AG's reasoning. Overall, the regulations provide some helpful clarification, but they also leave several issues unaddressed. Businesses should keep in mind the below summary of key provisions and comments from the AG as they prepare to implement the regulation's requirements.

Notice at Point of Collection

The regulations include useful guidance on how businesses can comply with the CCPA's notice requirement. First, the regulations provide illustrative examples of compliant notice for both on and offline practices. For example, businesses collecting personal information from consumers online may provide a "conspicuous" link to the notice on the business's homepage and on all webpages where personal information is collected and oral notice is permitted if a business collects personal information in person or over the phone.

Notably, in responding to comments in the final statement of reasons (FSOR), the AG states that the regulations "gives businesses discretion in determining how to provide the notice so that it is "made readily available where consumers will encounter it at or before the point of collection" of personal information."

Second, the last round of revisions clarified that a business that does not collect personal information directly from a consumer does not need to provide notice at collection to the consumer if it does not sell the consumer's personal information. Further, a data broker does not need to provide notice at collection if it has registered with the AG as a data broker and includes in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit an opt-out request.

Finally, notice and "explicit consent" is required where a business uses personal information for a purpose materially different from what was disclosed in the initial notice. "Explicit consent" is not defined and it appears distinct from the CCPA's "explicit notice" requirement. The AG has also not clarified what "explicit notice" means under the CCPA, which is required where a third party sells personal information that has been sold to it by a business.

Contact

Natasha G. Kohne
Partner
nkohne@akingump.com
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
+1 214.969.2713

Rachel Claire Kurzweil
Associate
rkurzweil@akingump.com
+1 202.887.4253

Shelly A. Kim
Associate
shelly.kim@akingump.com
+1.310.728.3333

But, in responding to comments in the FSOR on the lack of definition of “explicit consent”, the AG stated that “[b]usinesses have discretion to determine the manner in which to notify the consumer and obtain consent within the framework of the CCPA and the regulations.”

Privacy Policies

The regulations require that a privacy policy be posted online using a “conspicuous” link containing the word “privacy” on the business’s homepage or download page, landing page, or settings menu of a mobile application. Offline businesses must make the privacy policy conspicuously available to consumers. A privacy policy must also identify the categories of personal information the business has disclosed for a business purpose or sold to third parties in the preceding 12 months, and for each category of personal information identified, provide the categories of third parties to whom the information was disclosed or sold.

Requests to Know or Delete

The proper methods for submitting and responding to requests to know (RTK) or delete (RTD) depend on the operations of the business. In the last round of revisions, the AG clarified that while a business may not provide certain sensitive information in response to a RTK, including social security or financial account numbers, it is required to inform the consumer with “sufficient particularity” that it has collected specific sensitive information. A business need not search for personal information that is not maintained in a searchable or reasonably accessible format, maintained solely for legal or compliance purposes, and not sold, but must describe the categories of records it did not search under the foregoing exceptions.

Businesses may deny an unverifiable RTK or RTD and previous revisions clarify that a business may use a two-step process for online RTD, but that such process is not required. In response to a verified RTD, a business must permanently erase or deidentify that consumer’s personal information on existing systems or aggregate the consumer information. A business may offer the option to partially delete personal information, so long as it also offers the consumer the option of deleting all personal information.

Requests to Opt Out

A business must provide two or more methods for submitting opt-out requests, including a form titled “Do Not Sell My Personal Information,” or “Do Not Sell My Info,” accessible via a “clear and conspicuous link” on the website or mobile application. Notably, the regulations have removed all guidance from earlier drafts regarding a uniform opt-out button or logo. A consumer can also opt out by providing written permission to an authorized agent to submit a request on the consumer’s behalf, or by using user-enabled global privacy controls, when such signals are developed.

Service Providers

The regulations provide that “service providers” include entities directed by a business to collect information directly from or about consumers. Notably, while silent in the CCPA, the regulations make clear that service providers can disclose personal information to subcontractors that meet the service provider requirement under the CCPA.

After a number of iterations, the AG settled on language that allows service providers to use personal information to improve its services, but prohibits the service provider from using personal information to build or modify consumer profiles to provide services to another business or to correct or augment data acquired from another source.

Conclusion

Although some guidance remains unclear, businesses should review and implement the regulations to operationalize the CCPA before the AGO is authorized to enforce the CCPA, likely starting on July 1, 2020.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Author Information

Natasha G. Kohne is a partner at Akin Gump, where she is co-head of the firm's cybersecurity, privacy and data protection practice. She advises on privacy- and cybersecurity-related compliance, investigations and enforcement actions. She also represents companies in U.S., international and cross-border litigation, arbitration and investigations.

Michelle A. Reed is a partner at Akin Gump, where she is co-head of the firm's cybersecurity, privacy and data protection practice. Reed assists clients in conducting privacy and security risk assessments, as well as developing cybersecurity policies and procedures. She also represents clients in a variety of complex civil litigation matters.

Rachel Claire Kurzweil is an associate at Akin Gump, where she advises clients on privacy related compliance matters and on regulatory issues to clients in the health-care sector.

Shelly A. Kim is an associate at Akin Gump, where she advises clients on data privacy compliance matters, as well as complex commercial litigation and class action defense.

The authors wish to acknowledge the assistance and contributions of counsel Molly Whitman with this Insight.