

February 12, 2020

Not There Yet — California AG Publishes Modified Proposed CCPA Regulations

by Karen L. Neuman, Alex J. Moyer, Eric Dilulio

On February 7, 2020, the California Attorney General (AG) published, and updated on February 10, [modified proposed regulations](#) (Modified Regulations) implementing the California Consumer Privacy Act (CCPA). The Modified Regulations amend proposed regulations published by the AG in October 2019 (Initial Regulations) (see [here](#) for our alert on the Initial Regulations) in response to hundreds of comments submitted to the AG in December. The Modified Regulations were accompanied by a [Notice of Modifications](#) and a list of [Documents and Other Information Relied Upon](#). Written comments must be filed with the AG by February 25, 2020.

Among other changes, the Modified Regulations (1) narrow the scope of “personal information” under the CCPA; (2) clarify how service providers may use information processed as a part of their services; and (3) replace some onerous transparency and consumer rights request obligations with more practical requirements. Despite these changes, the Modified Regulations do not address a number of open questions, including, crucially, uncertainty about the scope of “sales” under the CCPA.

With the looming July 1, 2020 date for the start of enforcement by the AG, and a round of public comment on the Modified Regulations, companies hoping for clarity – and finality on the implementing regulations – may be disappointed.

The following is our analysis of the most significant features and changes in the Modified Regulations:

DEFINITION OF "PERSONAL INFORMATION"

The Modified Regulations clarify that determining if data is “personal information” depends on whether the business maintains the information in a manner that “identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.” For example, according to the Modified Regulations, collection of an IP address that is not linked, and could not reasonably be linked, to a particular consumer or household is not personal information.

This clarification will be a welcome change to businesses that collect IP addresses and little if anything else, and to businesses that use cookies and other automatic data collection technologies for website analytics and functionality but do not collect other information that could identify or reasonably be associated with a particular consumer or household. Importantly, information that is personal for one business may not be personal to a second business if the second business lacks the means of associating the information with an individual.

SERVICE PROVIDERS' USE OF PERSONAL INFORMATION

The Modified Regulations remove a provision from the Initial Regulations that prohibited service providers from using personal information received from one customer to provide services to another. There had been considerable opposition to this prohibition on grounds that it is not aligned with established market practice of providers seeking to build or improve the quality of their offerings.

Thus, the Modified Regulations provide that a service provider may use personal information obtained in the course of providing services for, among other administrative purposes, building or improving the quality of its services, provided that the use does not include (i) building or modifying profiles on consumers or households; or (ii) cleaning or augmenting data acquired from another source. While this change does not permit service

providers to use personal information for any and all internal purposes, it does allow most service providers to use personal information for product development and improvement, preventing significant disruption to current market practices and potentially removing barriers to innovation, for example, for companies training certain AI and machine learning algorithms.

PERSONAL INFORMATION COLLECTED FROM THIRD PARTIES

Under the Initial Regulations, a business that does not collect information directly from consumers that wanted to sell that information would have been required to (i) contact the consumer directly to give notice; or (ii) obtain an attestation from the source of the information. The Modified Regulations remove these requirements (which would have been virtually impossible for many businesses to comply with) if a business (i) registers with the AG as a “data broker” (see [here](#) for our previous alert on the data broker registration requirement); and (ii) includes in its registration a link to its privacy policy containing instructions on how to opt out.

PRIVACY POLICIES AND OTHER NOTICES

The Modified Regulations provide further guidance about the form and content of privacy policies and other CCPA notices. Businesses must still disclose in their privacy policies the categories of personal information collected, sold, and disclosed for a business purpose in the preceding 12 months, and the categories of third parties to whom that information was disclosed or sold. However, the previous requirement to disclose, for each category of information collected, the source and purposes of that collection has been removed. This change should streamline CCPA privacy disclosures consistent with trends in global privacy frameworks to keep privacy policies concise, and easy to read and understand.

The AG retained the recordkeeping and corresponding transparency requirements in the Initial Regulations for businesses that process a significant amount of personal information, but increased the threshold from 4 million to 10 million California residents (roughly equal to 25 percent of the state’s population). These metrics must be annually disclosed in their privacy policies or on their websites by July 1.

As [we have discussed previously](#), all CCPA-mandated notices must be accessible to consumers with disabilities. The Modified Regulations expand on this by requiring businesses posting notices online to follow generally recognized industry accessibility standards, such as the [Web Content Accessibility Guidelines](#). In addition, just-in-time notices (e.g., pop-up notifications) must be provided for collection of personal information from a consumer’s mobile device for a purpose that the consumer would not reasonably expect (e.g., collecting location information for a flashlight application).

CONSUMER RIGHTS REQUESTS

Businesses are no longer required to post an interactive webform to receive access or deletion requests, although this method may still be useful for businesses looking to standardize requests. While most businesses must still provide two or more designated methods to submit access and deletion requests, a business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information is only required to provide an email address for submitting access requests.

Interactive webforms, however, are still required for requests to opt out of sales. The methods for making these opt-out requests must “be easy for consumers to execute” and require minimal steps (although no further detail is provided on what is considered “easy”). This provision also prohibits using methods that would subvert or impair a consumer’s decision to opt out, presumably, for example, by implementing methods that are misleading or deceptive.

Importantly, the AG has retained and expanded on a provision in the Initial Regulations requiring businesses that collect personal information from consumers online to treat user-enabled global privacy controls as valid

opt-out requests. These controls (e.g., browser plugins or device settings) must clearly communicate or signal that a consumer intends to opt out of the sale of their personal information, and must require consumers to make an affirmative election rather than rely on pre-selected settings.

While the Modified Regulations dictate that these global privacy controls take precedence over business-specific settings, such as participation in a financial incentive program, they permit a business to notify a consumer of the conflict and give the consumer the choice to confirm the business-specific setting. These revisions may assuage some concerns raised in response to the introduction of this requirement in the Initial Regulations, but questions remain about how global privacy controls will be standardized and effectively implemented across the Internet.

CONCLUSION

Companies that are subject to the CCPA should review the Modified Regulations and assess the impact on their CCPA compliance strategies, and may want to consider submitting comments to the AG before the February 25 deadline. We are available to answer any questions you have about the Modified Regulations and can assist you with submitting written comments.

We will continue to monitor key developments and keep you updated.

Authors + Contacts:

[Karen L. Neuman](#)

[Alex J. Moyer](#)

[Eric Dilulio](#)

Goodwin's CCPA team includes [Karen Neuman](#), [Eric Dilulio](#), [Alex Moyer](#), [David Kantrowitz](#), [Jackie Klosek](#), [David Rouse](#) and [William Stern](#).

To learn more about how Goodwin can help your company address privacy and cybersecurity, contact [Brenda R. Sharton](#), partner and Chair of the [Privacy & Cybersecurity](#) practice, or [Karen L. Neuman](#), partner and privacy lead, [Privacy & Cybersecurity](#) practice in Washington, DC.

Goodwin's *Chambers* and *Legal 500* ranked Privacy & Cybersecurity practice offers a fully integrated, multi-disciplinary approach to clients' data protection needs. One of the longest-standing of any Am Law 50 firm, our global team is uniquely positioned to provide the most innovative solutions to guide clients through the collection, use, processing and protection of their most sensitive information. Our senior lawyers include the former Chief Privacy Officer of the U.S. Department of Homeland Security in the Obama administration and internationally recognized privacy practitioner, a *Legal 500* "Leading Lawyer" and a "Next Generation Lawyer" in Cyber Law and Data Breach Response, as well as four other *Legal 500* Cyber Law ranked partners, several former federal prosecutors, and multiple FTC, GDPR, CCPA, HIPAA, GLBA and COPPA experts. We have handled hundreds of data breaches, including high-profile, global incidents involving everything from ransomware to nation-state attacks; have advised on over 700 public and private transactions in the last year alone; and have designed practical solutions and strategic privacy, information security and compliance programs for startups, global enterprises, and everything in between. We have litigated landmark privacy cases and defended against class action and government enforcement actions brought by the FTC, OCR/HHS, state attorneys general and regulators across the globe.

CONTACTS:

Notices

Karen L. Neuman

Partner

+1 202 346 4039

kneuman@goodwinlaw.com

Alex J. Moyer

Associate

+1 202 346 4257

amoyer@goodwinlaw.com

Eric Dilulio

Associate

+1 650 752 3140

edilulio@goodwinlaw.com

© 2020 Goodwin Procter LLP. All rights reserved. This informational piece, which may be considered advertising under the ethical rules of certain jurisdictions, is provided with the understanding that it does not constitute the rendering of legal advice or other professional advice by Goodwin Procter LLP, Goodwin Procter (UK) LLP or their attorneys. Prior results do not guarantee similar outcome.

Goodwin Procter LLP is a limited liability partnership which operates in the United States and has a principal law office located at 100 Northern Avenue, Boston, MA 02210. Goodwin Procter (UK) LLP is a separate limited liability partnership registered in England and Wales with registered number OC362294. Its registered office is at 100 Cheapside, London EC2V 6DY. A list of the names of the members of Goodwin Procter (UK) LLP is available for inspection at the registered office. Goodwin Procter (UK) LLP is authorized and regulated by the Solicitors Regulation Authority.

IRS Circular 230 Disclosure: To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. tax advice contained in this informational piece (including any attachments) is not intended or written to be used, and may not be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.