THOMSON REUTERS

Westlaw®

Q&A: Odia Kagan on the CCPA's draft regulations

By Jason Seashore, J.D.

MARCH 20, 2020

(March 20, 2020) - Fox Rothschild LLP partner Odia Kagan, who focuses on international privacy and compliance with the EU General Data Protection Regulation, answers Thomson Reuters' questions about the draft regulations of the California Consumer Privacy Act.

Thomson Reuters: On Feb. 7 the California attorney general proposed amendments to the California Consumer Privacy Act's draft regulations, and he released a second set of modified regulations March 11. What are your key takeaways?

Odia Kagan: My key takeaways are:

Highlight on transparency

- The regulations emphasized the requirement for the four different privacy notices (notice at collection, notice of opt-out, notice of financial incentive and general privacy notice). Looks like those four are here to stay.
- Disclosure of sources of information and third parties with whom information is shared with enough particularity to provide consumers with a meaningful understanding of the type of person or entity.
- Do-not-sell notice: A business that collects personal information through a mobile application may provide a link to the notice within the application, such as through the application's settings menu.
- If you collect personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, you need to provide a just-in-time notice (e.g., a pop-up) containing a summary of the categories of personal information being collected and a link to the full notice at collection.
- The notice needs to be provided in an accessible manner. This version of the regulations specifically mentions the WCAG2.1 accessibility standard.
- Granular disclosure by category: The requirement to list sources and purposes of use by specific category seems to have been removed. However, there is still an obligation to disclose information shared with third parties by specific category.
- New regs from March 11 added back the requirement to include in the privacy notice categories of sources from which the personal information is collected and the purpose for which it was collected.

Opt-out

The second regs added a proposed opt-out logo and button. Following very strong criticism about the format of the button being misleading and not effective, the third version of the regs removed the suggested button.

IP address

The second draft of the regs added a provision, pursuant to which, under certain circumstances, an IP address may not constitute personal information. This put in question some application of the CCPA to cookies and adtech and raised questions as to how it should be interpreted. The third draft of the regs removed this provision.

Service providers

The second and third drafts expand the uses that service providers may make of personal information provided by the businesses. Of particular note:

- Service providers may retain personal information to process or maintain personal information on behalf of the business that provided the personal information, or that directed the service provider to collect the personal information, and in compliance with the written contract for services.
- Service providers may also retain personal information for internal use to build or improve the quality of their services, provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business, or correcting or augmenting data acquired from another source.

TR: How do the proposed amendments streamline requirements for companies selling information they did not collect directly from consumers, and how is California's broker registration law implicated?

OK: The new regulations did away with the requirement found in the original regulations, that in order to sell information not collected directly from individuals, companies (data brokers) would need to either contact the consumer directly and provide notice and opt-out or contact the source and receive an attestation that such notice had been provided.

This was a very burdensome requirement because data brokers, by definition, do not have a direct relationship with third parties and thus, reaching out to such parties is either impossible (the data broker does not have the person's contact info at all) or expensive (the data broker only has a postal address).

In place of this requirement, the new regulations say that a data broker is not required to provide a notice at collection if it is registered with the attorney general as a data broker pursuant to the California broker registration law and has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out.

This puts the disclosure on the data broker's website as a replacement for contacting the individual directly and greatly simplifies the process for data brokers engaging in internal processing of data collected indirectly. The third version of the regs clarified that if you do not collect information directly from consumers and do not sell it, you do not need to provide a notice at collection.

However, the requirements change when they intend to sell the information. In this context, the new regulation note (in 999.306(e)) that "A business shall not sell the personal information it collected during the time the business did not have a notice of right to opt-out notice posted unless it obtains the affirmative authorization of the consumer" reinstates the requirement for affirmative consent and reaching out to the individual where an opt-out notice was not in place for the information that the data broker contemplates selling.

TR: What are the new just-in-time privacy notices for unexpected mobile device data collection?

OK: The regulations require that if you collect information for use that would be unexpected for the consumer, you need to add a just-in-time notice in order to alert the consumer of this fact. They give an example which was actually the object of an FTC enforcement action, namely a flashlight app for a mobile device that also collects geolocation information.

Generally speaking, precise location is something that consumers do not usually expect, and the FTC has flagged this as sensitive information before. Generally speaking, the regulations take the position (echoed in GDPR and other laws) that, especially for unexpected data collection or processing, putting information as part of a general privacy notice that is located on a website is not enough to achieve sufficient transparency.

TR: What ambiguity still exists in the regulations following the proposed amendments which will likely need clarification down the road, either in terms of further modifications or litigation?

OK: As we can see from the third revision that came out March 11, there are still areas that need clarification. They include:

- The opt-out button — what it should look like and how to operationalize it.
- Financial incentive — how does calculating the value work in real life and how should businesses address it?
- Liability of businesses for the actions of third parties, i.e., what does "had reason to believe" mean in real life?

TR: The regulations will likely not be finalized until shortly before the CCPA enforcement deadline of July 1. What are your thoughts on the recommendation of Santa Clara University professor and privacy expert Eric Goldman that the California Justice Department should announce a grace period to give businesses adequate time to comply with the final regulations?

OK: Professor Goldman is joined in this plea by other parties that submitted comments to the regulations. The reasoning behind this is that both sets of regulations contain substantial changes from the original language of the law and imposed additional obligations.

Each such change requires companies to revisit their compliance efforts and change them, and they often need to change privacy notice language, language of agreements with service providers, methods for submitting requests, etc.

A lack of certainty in the language of the law makes it difficult for companies to comply. If the next version of the regulations will include additional changes, there will be very little time left for companies to carry out additional changes before the law becomes effective in July.

TR: What are your reactions to the first lawsuit alleging violations of the CCPA: *Barnes v. Hanna Andersson LLC*, No. 20-cv-812, *complaint filed*, 2020 WL 1026619 (N.D. Cal. Feb. 3, 2020)?

OK: This is the start of many cases that will help provide a strong definition of what are the "reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure" that the CCPA requires companies to implement.

To date, no official definition has been given, and companies would turn to criteria set forth by FTC publications and consent orders, NIST or ISO standards and the CIS Top 20. As litigation under the CCPA starts, we will get more clarity on this from the courts.

In this case, the complaint seeks a declaratory judgment that the defendants' existing security measures do not comply with its duties of care to provide reasonable security procedures but does not yet seek statutory damages under the CCPA.

If the plaintiff can establish that the security procedures and practices implemented by the respondents were not reasonable, the plaintiff will likely amend the complaint seeking statutory fines that are provided for under the CCPA.

TR: Since we're talking about California privacy law, any thoughts on the proposed Genetic Information Privacy Act currently being considered by the state Legislature? Given that the CCPA already addresses the processing of biometric information (including DNA), what would the GIPA add to the regulatory mix?

OK: The GIPA goes further to restrict use of genetic information in ways that use of personal information (including biometric) under the CCPA are not limited.

The GIPA goes further in four ways:

- The GIPA would require written opt-in consent for any disclosure of genetic information to a third party, whereas the CCPA requires for a sale of information, a notice plus opt-out.
- The GIPA would limit the use of genetic information to the purpose specifically authorized by the individual to whom it pertains, whereas the CCPA, in the amended regulations, prohibits uses for another purpose only if it is materially different than the disclosed purpose.
- The GIPA would require destruction of the information as soon as this purpose is achieved, whereas the CCPA does not impose any requirements regarding data minimization and only requires deletion pursuant to a deletion request, which is subject to a number of exceptions including internal uses that are compatible with a purpose expected by the individual.
- Depending on the circumstances, the GIPA would impose criminal as well as civil liability for violations.

This article first appeared in the March 20, 2020, edition of Westlaw Journal Computer & Internet.

ABOUT THE AUTHOR

Odia Kagan is partner and chair of the GDPR Compliance & International Privacy practice at **Fox Rothschild LLP** in the firm's Philadelphia office. She advises clients on how to design and implement their products and services, consummate their M&A transactions, and engage third-party vendors in the United States and abroad. Odia has assisted more than 80 companies, from U.S.-based multinationals to startups, on their path to compliance with the EU General Data Protection Regulation. She can be reached at okagan@foxrothschild.com.