ACC DOCKET

INFORMED. INDISPENSABLE. IN-HOUSE.

A Dedicated Data Discussion

Technology, Privacy, and eCommerce

This past year, the world saw a tremendous amount of activity around personal data privacy, especially the United States. As a lawyer specializing in data privacy, even I find it hard to be aware of the specifics when this area moves so quickly. With that in mind, ACC has devoted space in the Docket to keeping its members abreast of the latest data developments with this new column.

Amid the new US laws and amendments, from Hawaii to Connecticut and North Dakota to Texas, none were as broad and far-reaching as California’s Consumer Privacy Act (CCPA). Under CCPA, California residents will have the right to know what personal data is collected about them and how it is used. Businesses that collect consumer data, operate in California, and meet one of the following criteria: have annual gross revenue of US$25 million; or possess the personal information of 50,000 or more consumers, households, or devices; or earn more than half their annual revenue from selling personal data need to comply with CCPA. The law is expected to serve as a model for other states and nations, so in-house counsel who are not currently affected should follow its developments with an eye toward their own jurisdiction.

Although many companies have been preparing for the CCPA for months, it is important to remember that the law is still subject to some final clarifications that were proposed in October 2019.

The most important recent amendments provide a one-year moratorium on most provisions for applicant/employee data and B2B data. The legislature intends to pass laws addressing these two categories of data during the 2020 session. If not, or if the sunset provision is not extended, both sets of data will once again be subject to the full force of the CCPA. Another important amendment clarifies that aggregated or de-identified data does not qualify as personal data and neither do data sets published by the government.

In addition, the proposed regulations address other major topics, such as the following.

Notices to consumer

Where businesses provide materials in a particular language, the notice should be in the same language. For example, if a business with a large Spanish-speaking consumer base provides resources in Spanish, the notice about privacy should also be in Spanish. Notices should also be available for individuals with disabilities. When it comes to selling data acquired through a third party, businesses must obtain an attestation from the third party that the data may be sold. Businesses also need to provide notices for offline activity. Instructions for when and how to provide notice of financial incentives are outlined. Lastly, the regulations address how to construct a notice and when and how it should be presented to a consumer.

Handling consumer requests

The law requires two methods for consumers to request rights unless the business is only online, in which case there are other methods (e.g., forms in person). For deletion requests, there should be a two-step process (request and confirm). In some cases, consumers may submit requests in a way the business isn’t prepared for. Businesses need to verify the request, and if they cannot, there is guidance on next steps.

Once a request for deletion is to be granted, businesses may purge the data by deleting it or by de-identifying or aggregating the information. The consumer needs to be informed of how their data was deleted. Importantly, the regulations address the technical difficulty of deleting from backups. Businesses do not need to delete from backups until the backups are used. If, however, a business offers a requester an option to only delete some of the data, the option to delete all data must be more prominent than other options. No matter what, all actions, options, exceptions, and decisions must be communicated to the requester.

The regulations provide clarification on opting out of data-selling mechanisms. Options for opting out of all or some must include the prominent choice of a global opt-out, and that the request need not be verifiable, merely good faith and documented belief of identity. However, opt-in (again) requests should be a two-step process: request and confirm.

Records on requests shall be retained for 24 months. Businesses that annually buy/sell/share data on four million or more consumers for commercial purposes must report metrics on requests and type of response by request type and the timeframe to complete the request — and then post the metrics publicly. Household requests may be completed in aggregate unless the business can individually verify the identity of all members of the household and they all make the request.

Verification of requests

Where possible, businesses will use existing data to verify identity and will take a reasonable, risk-based approach to verification needs. Businesses should avoid collecting new data. If they need to do so, it should only be for identity verification and promptly deleted. Fraud detection measures should be used. A pre-existing password protected account can be used for verification purposes unless the business suspects fraud.

The regulations also address the number of verification items required in response to the level or type of request. Categories of data require two identity verification items, whereas a request for pieces of specific information require three items and a signed declaration of identity under penalty of perjury. If a business cannot verify identity for types of information it collects, it should state so in the privacy notice.

If someone is authorized to act on behalf of another person, proof of authorization and proof of identity of the person is required unless the authorization is a power of attorney.

Nondiscrimination

The regulations provide several examples and indicate that denying a consumer's request or charging fees to fulfill requests where permitted by law are not considered discriminatory practices. This section also provides methods for businesses to calculate the value of the consumers' data.

Interactions with other laws

There are some specific interactions with other laws within the CCPA, both state and federal. On the federal level, the CCPA (under 1798.145) does not apply to:

- Medical information governed by the Confidentiality of Medical Information Act or Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act of 1996 (along with its subsequent amendments, HIPAA);
- A provider of healthcare governed by the two laws above, to the extent they maintain patient information in the same manner as medical information or PHI (as described above);
- Clinical trial information under the Common Rule or the US Food and Drug Administration (FDA);
- Consumer credit report information under the Fair Credit Reporting Act (FCRA) with noted recent amendments above;
- Information under the Gramm-Leach-Bliley Act (GLBA), or the California Financial Information Privacy Act; and
- Information under the Driver's Privacy Protection Act of 1994.

What does this mean for in-house counsel?

When considering privacy compliance, there are some impacts on in-house counsel that are standard across privacy laws. Areas likely to be affected include vendor management and contractual obligations, data inventory purpose and legal bases data collection, online/external privacy notice, and internal policies, among others. Legal should identify its role in incident response management and assist with development of an individual rights management program. In addition, counsel should stay current on applicable requirements that affect company or data being processed and make sure that the implicated departments are aware of their privacy compliance needs.

K Royal

Global Chief Privacy Officer

Crawford & Company

K Royal earned her JD from the Sandra Day O'Connor College of Law at Arizona State University.

She also holds a PhD in Public Affairs from the University of Texas at Dallas.

Reach out to K about her column at @heartofprivacy on Twitter, or www.linkedin.com/in/kroyal/.