CARLTON FIELDS

It’s 3 a.m., Do You Know Where Your Data Is? The Importance of Data Mapping and the California Consumer Privacy Act

CYBERSECURITY AND PRIVACY | JULY 29, 2019

Joseph W. Swanson

The California Consumer Privacy Act (CCPA) takes effect in January and imposes a number of requirements on how businesses collect, use, and transfer personal information. Among other things, a business subject to the CCPA must be able to respond to consumers' requests for information about what personal information the business collects and whether the business sells that information. Businesses must also provide the consumer’s personal information to that individual and delete it if requested to do so.

The California attorney general is authorized to enforce the CCPA. In addition, the CCPA provides a private right of action — with statutory damages of $100 up to $750 per consumer per incident — for data breaches caused by a business’s failure to implement reasonable security measures.

Given those stakes, organizations that do business in California and that collect personal information relating to California residents need to prepare for the law’s onset. The myriad obligations created by the CCPA, and the fact that those obligations do not neatly align with those created by the EU’s GDPR and other privacy regulations, may seem overwhelming to businesses.

But those organizations can attack compliance in a disciplined manner by asking themselves some threshold questions: *What personal information do we collect, where is it stored, and what do we do with it?* These questions are part of a process called “data mapping,” in which an organization evaluates the data it collects, where it is stored, and how (if at all) it is shared with third parties. This process is essential for an organization to be able to act on a consumer’s request related to his or her personal information under the CCPA.

A business that has previously engaged in data mapping can and should leverage that earlier work, but the organization should be mindful of some unique aspects of the CCPA. First, the CCPA defines “personal information” to include some relatively novel items, such as biometric information, education information, geolocation information, and household information. And, second, the CCPA defines the “sale” of personal information to include selling, transferring, or communicating that information to a third party for money or “other valuable consideration.” Given the breadth of these definitions, a business engaged in data mapping for the CCPA should consider whether to supplement previous data mapping that may not have incorporated these concepts. And, some organizations may find themselves data mapping for the first time.

A business can deploy its own resources and/or work with third-party service providers to complete data mapping. If using a third party to assist, the business may want that third party retained by counsel so as to better protect the work under the attorney-client privilege. The business should document its data mapping so that there is a defensible record of its attempts to comply with the law. That record will also be helpful when updating the data mapping in the future, as other jurisdictions will inevitably pass additional CCPA-like provisions.

views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.