The Washington Privacy Act – Re-Introduced for 2020 – Is it the Best of CCPA and GDPR?

Robinson+Cole

Article By
Deborah A. George
Robinson & Cole LLP
Data Privacy + Security Insider

- Civil Rights
- Communications, Media & Internet
- Administrative & Regulatory
- California
- Washington

Wednesday, February 12, 2020

Washington legislators recently introduced the Washington Privacy Act (WPA). This legislation is a consumer-focused privacy law similar to the California Consumer Privacy Act (CCPA) but it also has some EU General Data Protection Regulation (GDPR)-like concepts. The WPA protects personal data in much the same way as CCPA, but with some significant differences. The WPA applies to legal entities that conduct business in Washington or produce products or services that are targeted to residents of Washington, and that satisfy one or more of the following thresholds:

(a) Controls or processes personal data of one hundred thousand consumers or more;
(b) Derives over fifty percent of gross revenue from the sale of personal data and processes or controls personal data of twenty-five thousand consumers or more.

The WPA applies only to consumers and, as drafted, the legislation states that the definition of consumer does not include a person acting in a commercial or employment context. The WPA also does not apply to protected health information under the Health Insurance Portability and Accountability Act (HIPAA), activities governed by the Fair Credit Reporting Act, personal data collected pursuant to the federal Gramm-Leach-Bliley Act, the federal driver’s privacy protection act, several other federal and state laws, and data maintained for employment records purposes.
There are also some differences between the WPA and the CCPA including a consumer right to correction of data, which is not available in the CCPA. The WPA introduces the concept of data minimization and limits data collection to what is relevant and reasonably necessary for the specific purpose for which the data was collected. The WPA contains similar language to GDPR regarding the concept of data controllers and processors and data protection assessments. The WPA requires a data controller to conduct data processing assessments for each processing activity that involves personal data. The WPA does not include a private right of action like CCPA, and leaves enforcement of the WPA exclusively to the Washington state Attorney General.

Unlike either CCPA or GDPR, the WPA also includes provisions regarding facial recognition technology. Some notable provisions with respect to facial recognition technology require that controllers using facial recognition technology must provide a conspicuous and contextually appropriate notice whenever facial recognition service is deployed in a physical premise open to the public that includes, at minimum:

(a) The purpose or purposes for which the facial recognition service is deployed; and
(b) Information about where consumers can obtain additional information about the facial recognition service including, but not limited to a link to any applicable online notice terms or policy that provides information about where and how consumers can exercise any rights that they have with respect to the facial recognition service.

The WPA also requires controllers to obtain consent from a consumer prior to enrolling an image of that consumer in a facial recognition service used in a physical premise open to the public. Processors that provide facial recognition services must prohibit, in any written contract for such services, the use of facial recognition services by controllers to unlawfully discriminate under federal or state law against individual consumers or groups of consumers.

Copyright © 2020 Robinson & Cole LLP. All rights reserved.