Washington State Considers Consumer Privacy Bill with Controversial Enforcement Provision

Friday, March 20, 2020

Never a dull moment for consumer privacy law, as we get deeper into 2020. With the California Consumer Privacy Act (“CCPA”) in full effect, states across the nation are scrambling to develop their own version of this groundbreaking law, and leading the pack has been the state of Washington. In 2019, a group of state senators in Washington introduced the Washington Privacy Act (“WPA”), which passed unanimously in the state Senate, but ended up stalling in the house. Now, in 2020, the WPA bill has been revived by state Senator Reuven Carlyle, in a slightly updated version that Senator Carlyle is confident will fare better in the legislative process.

“This year, after months and months of extraordinary amounts of stakeholder work, relationships, extensive conversations, iterations of various versions of the bill, we have overwhelming consensus that we need to move forward and we have about, I would say, 95% agreement in principle on the core elements of the bill,” Carlyle stated in a
press conference announcing the bill, back in January.

Unlike other states that are modeling their bills largely on the CCPA, the WPA would establish more GDPR-like requirements on businesses that collect personal information related to Washington residents. In fact, the WPA’s legislative findings explicitly state that in absence of federal standards, Washington and other states are “analyzing element’s of the European Union’s GDPR” to inform their own state consumer privacy measures. In addition to requirements for notice, and consumer rights such as access, deletion, and rectification, the WPA would impose restrictions on use of automatic profiling and facial recognition.

Below are key aspects of the WPA:

- **Jurisdictional Scope.** The WPA would apply to legal entities that conduct business in Washington or produce products or services intentionally targeted to residents of Washington, and that satisfy one or more following thresholds: Controls or processes data of 100,000 consumers or more; or Derives over 50% of gross revenue from the sale of personal information and processes or controls personal information of 25,000 consumers or more. The bill includes exemptions for personal data regulated by HIPAA, HITECH, GLBA, FERPA and data maintained for employment record purposes. Personal data is defined vaguely to include “any information relating to an identified or identifiable natural person”.

- **Consumer Rights.** Washington residents would be afforded a broad set of rights in respect to their personal data:
  - **Right to access** – A consumer would have the right to confirm whether or not a controller is processing personal data concerning the consumer and access that personal data.
  - **Right to correction** – A consumer would have the right to correct inaccurate personal data concerning the consumer, taking into account the nature of the personal data and the purposes of the processing of the personal data.
  - **Right to deletion** – A consumer would have the right to delete personal data concerning the consumer.
  - **Right to data portability** – A consumer would have the right to obtain their personal data in portable, to the extent technologically feasible, a readily usable format allowing consumers to transport that data.
  - **Right to opt out** – A consumer would have the right to opt out of personal data processing for purposes of targeted advertising, sale of personal data, profiling, or other similar measures.

- **Controllers and Processors.**
  - In general, controllers determine the purposes and means of processing personal data, while processors process personal data on behalf of the controllers. Thus, under the WPA, controllers would be responsible for meeting the requirements of the WPA, while processors are responsible for
following the instructions of their controllers and assisting them with meeting the requirements of the law. Contracting between the parties will be critical.

- Controllers must be transparent and accountable for processing of personal data by making a “meaningful,” “clear,” and “reasonably accessible” privacy notice available. Notice must include: the categories of personal data collected, the purpose for which personal data is disclosed to third parties, the rights the consumer may exercise, the categories of personal data shared with third-parties, the categories of third-parties with whom the controller shares data.

- **Data Protection Assessments.** Controllers must conduct and document a data protection assessment of their processing activities involving personal data including: processing for purposes of targeted advertising, sale of personal data, profiling, processing of sensitive data, and processing of personal data that presents a heightened risk of harm to the consumer.

In a vote on February 14, the Washington state Senate voted 46-1 to pass the WPA. However, in the WPA’s latest round of review, on February 28, by the House Innovation, Technology, Economic Committee, committee chairman Zach Hudgins (D) introduced a controversial amendment to the bill. To this point, in all versions of WPA the Washington Attorney General was given exclusive enforcement authority. Senator Hudgins’ amendment would effectively provide consumers with a private right of action if a controller or processor breached any of the privacy requirements established by the WPA. Comparatively, the CCPA provides for a private right of action in limited circumstances related to a data breach due to a business’s failure to implement and maintain reasonable security procedures. A broad private right of action, as Senator Hudgins suggested, has been a point of contention for both federal and state legislatures considering consumer privacy measures, as such a provision would open the floodgates to class action litigation, and face significant backlash by industry leaders. The House approved the amended version of the WPA on March 6, however, the Washington state senate has refused to concur with Senator Hudgins amendment. As such, the House and Senate will now need to negotiate to determine if a compromise may be reached to allow the WPA to pass.

States across the country are contemplating ways to enhance their consumer privacy and security protections, and Washington is at the forefront. Organizations, regardless of their location, should be assessing and reviewing their data collection activities, building robust data protection programs, and investing in written information security programs (WISPs).

Jackson Lewis P.C. © 2020