Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Washington State Lawmakers Divided Over Private Right of Action and Other Relief in Dueling Data Privacy Bills

February 18, 2020

Key Points

- The Washington state Senate has passed its version of a consumer data privacy bill as state lawmakers debate proposed legislation for the Washington Privacy Act, the state's first data privacy law.
- In their own bill, House lawmakers have proposed significantly more expansive relief than the Senate, including a private right of action with statutory penalties of up to $50,000 for each violation and up to $100,000 for an intentional violation.
- The divergent approaches raise questions as to whether Washington will be able to pass a data privacy law in 2020 and overcome the divisions that sank its efforts to do so in 2019.

On February 14, 2020, the Washington state Senate passed Senate Bill 6281, bringing Washington one step closer to enacting the Washington Privacy Act, the state's first consumer data privacy law. In January, lawmakers introduced and began debate on companion bills in both houses of the state legislature. However, on February 7, 2020, House lawmakers proposed new language for their version of the bill—House Bill 2742—evidencing their intent to push for much further reaching relief than their Senate counterparts and creating uncertainty as to whether the state will reach consensus on the law's provisions. Notably, despite similar efforts in 2019, Washington failed to pass a privacy law after the version almost unanimously approved by the Senate failed to gain traction in the House. The Senate's version of the bill has now been introduced for debate in the House.

Below we compare key aspects of SB 6281 and HB 2742 and identify issues to watch as Washington seeks to pass its privacy bill into law.

Consumer Data Privacy Rights

As proposed, both SB 6281 and HB 2742 provide consumers with five core rights regarding data privacy:

Contact Information

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Anthony T. Pierce
Partner
apierce@akingump.com
Washington, D.C.
+1 202.887.4411

Melissa D. Whitaker
Counsel
mwhitaker@akingump.com
Washington, D.C.
+1 202.887.4538

1. Right to access personal data and to determine whether the consumer's personal data is being processed;
2. Right to correction of inaccurate data regarding the consumer;
3. Right to deletion of personal data;
4. Right to data portability of personal data regarding the consumer;
5. Right to opt out of data processing.

Yet key differences have emerged in how the two houses would interpret the scope of these rights. For instance, the Senate bill would limit the right to opt out of data processing only to circumstances involving targeted advertising, the sale of personal data or certain types of data profiling that affect benefits like housing, healthcare or employment opportunities. The House bill would permit consumers to opt out of data processing for any reason.

Unlike the Senate bill, the House bill would require controllers to not only process requests to enforce these rights internally, but also to pass on consumer requests to third parties to whom the controller has disclosed the consumer's information within the past year. Further, while the Senate would provide controllers with 45 days to respond to consumer requests regarding these rights, the House would offer only 21 days.

Scope of Application

Both houses agree that the law would apply only to legal entities that conduct business in Washington or target products or services toward Washington residents. Both bills also carve out specific exemptions for state and local governments, municipal corporations, health information subject to the Health Insurance Portability and Accountability Act (HIPAA), consumer credit reporting information, information subject to the Federal Education Rights and Privacy Act (FERPA) or the Gramm-Leach-Bliley Act, and information gathered for certain research purposes.

Narrowing its scope further, the Senate bill restricts application to only those entities that (1) control or process the personal data of at least 100,000 consumers in a calendar year **or** (2) derive more than 50% of gross revenue from the sale of such data while also controlling or processing the personal data of at least 25,000 consumers.

The proposed House bill would cover a much wider swath of entities. Companies will fall within the House bill's scope unless they (1) have fewer than ten employees; (2) enjoy gross annual revenues of less than $5 million; (3) derive less than 5% of gross annual revenue from the monetization of personal data; (4) control or process personal data for fewer than 20,000 consumers; **and** (5) restrict their use of personal consumer data to what is necessary to provide requested services and products to consumers.

Effective Date

Under either bill, the law would take effect on July 31, 2021.

Definition of Sale

The definition of "sale" has been the source of key debate in both houses. In its current form in SB 6281, "sale" is defined as "the exchange of personal data for monetary or

other valuable consideration by the controller to a third party." The House has proposed to modify the Senate's definition by adding in text that largely mirrors the California Consumer Privacy Act (CCPA) definition, to include selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating personal data for a commercial purpose to third parties.

Both bills exempt a range of activities from the definition of sale, including the disclosure of data publicly posted by consumers on mass media or the disclosure of personal data to a third party in direct relationship with the consumer for purposes of providing a requested product or service.

Private Right of Action and Preemption

SB 6281 does not include a private right of action. Enforcement is to be undertaken exclusively by the Washington Attorney General, and civil penalties for each violation may not exceed $7,500. Further, the bill would preempt any local law or ordinance regarding personal data processing.

Although initial versions of HB 2742 excluded a private right of action, House lawmakers have now rejected the Senate's approach and introduced a private right of action into their bill. Under the new provisions, non-compliant entities would be deemed to commit an unfair or deceptive business practice under the Washington Consumer Protection Act, through which consumers could bring a civil action for damages. Companies would be liable for up to $50,000 per violation and up to $100,000 for each intentional violation. Unlike the Senate bill, HB 2742 would not preempt localities from enacting their own laws and ordinances to regulate facial recognition technology.

As currently drafted, HB 2742 provides by far the highest amount of statutory monetary penalties in U.S. data privacy legislation that includes a private right of action. While the CCPA includes a private right of action, it caps consumer damages at $750 per incident. In 2019, Massachusetts proposed its own legislation with a private right of action, but limited damages to $750 per incident or actual damages, whichever is greater.

Loyalty Programs

As with the CCPA, trade and consumer groups presented concerns about the routine commercial practice of providing special discounts and offers to consumers who enroll in and provide personal data to companies through loyalty programs. Those groups feared that such programs would run afoul of the bills' prohibition on discriminating against consumers who exercise their rights as provided in the data privacy law. To address these concerns, SB 6281 and HB 2742 have each included an explicit exemption for "voluntary participation in a bona fide loyalty rewards" or discounts program.

Facial Recognition Technology

Stakeholders from Microsoft to the ACLU have presented comments on the state's controversial efforts to regulate the use of facial recognition technology through this legislation. Many commenters have focused on whether and how to impose testing thresholds for accurate facial recognition results as well as raising concerns about reliability when applying the technology to various genders and races. Stakeholders

have called on both houses to strike these provisions from the bill and separately regulate commercial facial recognition technology.

We will continue to closely monitor how these issues shake out for Washington and whether the state is ultimately able to enact a data privacy bill into law.

akingump.com