wiley

NEWSLETTER

Recapping Washington State's Privacy and Facial Recognition Bills

March 2020

Privacy in Focus®

This year, Washington state again tried to enact the nation's second comprehensive state privacy law, following California's Consumer Privacy Act. Last week, the legislature failed to come to agreement on SB 6281, a bill which would have had extensive effects on businesses operating in Washington. In this article, we look at the lessons for privacy regulation in Washington going forward, as well as a separate privacy law that *did* pass, SB 6280, governing the use of facial recognition services by state and local government agencies, which has now gone to the Governor for approval.

1. What SB 6281 Would Have Done.

Scope

SB 6281, if passed, would have covered "legal entities that conduct business in Washington or produce products or services that are targeted to residents of Washington," *and either* (1) control or process the personal data of 100,000 customers or more; *or* (2) derive over 50% of their gross revenue from the sale of personal data *and* process or control the personal data of 25,000 customers or more. The bill contained specific carveouts for governmental entities, organizations already regulated under federal privacy laws, and other enumerated categories of information, such as "[d]ata maintained for employment records purposes."

SB 6281 defined three broad categories of entities: processors, controllers, and consumers. *Processers* were defined as entities that "process"—*e.g.*, collect, use, store, analyze—data on behalf of a

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Boyd Garriott
Associate
202.719.4487
bgarriott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

controllers. *Controllers* were defined as entities that "determine[] the purpose and means of the processing of personal data." *Consumers* were defined as residents of Washington state.

The bill would have regulated several categories of data in different ways. The bill broadly governed "personal data," which it defined as "any information that is linked or reasonably linkable to an identified or identifiable natural person." It also placed additional restrictions on processing "sensitive data," which is "(a) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sexual orientation, or citizenship or immigration status; (b) the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; (c) the personal data from a known child; or (d) specific geolocation data." That said, the bill contained exemptions for deidentified data, pseudonymous data, and publicly available information.

Rights & Obligations

The basic structure of SB 6281 would have granted consumers specific rights and imposed obligations on businesses to operationalize consumers' use of those rights. In particular, consumers would have been guaranteed five rights that, pursuant to the bill, could not be waived or abrogated by any contractual provision:

- Access;
- Correction;
- Deletion;
- Portability;
- Opt out.

The right of *access* and *deletion* would have been relatively straightforward: they allowed consumers to access and delete personal information held by businesses. The other rights were more complicated.

The right to *correction* granted consumers 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." This provision would have raised several interpretive questions. For example, businesses may have had to determine what was necessary to verify that the consumer's "corrected" information was indeed correct. Additionally, the reference to the "nature" and "purposes" of the data appeared to make this right contextual, rather than a right that a consumer could invoke in all circumstances.

The right to *data portability* granted consumers the right to obtain personal data they provided to a controller in a "readily usable format that allows the consumer to transmit the data to another controller without hindrance," so long as (1) doing so was technically feasible, and (2) "the processing [wa]s carried out by automated means."

The right to *opt out* was specifically the right to opt out of "the processing of [a consumer's] personal data" when the processing was done for three discrete purposes: (1) targeted advertising, (2) the sale of personal data, and (3) "profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer." The bill defined the last category to mean "decisions that result in the provision or denial of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water."

The law also imposed obligations on processors and controllers. To effectuate consumer rights, controllers would have been required to respond to any consumer requests regarding one of their five rights within 45 days. That period could have been extended "where reasonably necessary," but consumers would have been able to challenge delays through an internal appeal process that the law required controllers to establish. Unless consumer requests were "manifestly unfounded or excessive," controllers were required to act upon these requests "free of charge" and "up to twice annually[.]"

Controllers also would have been required to comply with a number of provisions regarding transparency and handling of data, including:

- Maintaining a "reasonably accessible, clear, and meaningful private notice" explaining, among other things, what data the controller processes, why it does so, and how consumers may make their data requests;
- Limiting collection and use of personal data to what is "reasonably necessary" and "relevant" for the purposes of processing;
- Maintaining "reasonable" data security measures;
- Nondiscrimination in the processing of data;
- Refraining from processing any sensitive data, as defined by the bill, without obtaining consent;
- Conducting "data protection assessments" evaluating how data is processed and used.

Many of these additional obligations would have been substantial. In particular, the "data protection assessments" required businesses to consider whether their data processing "present[ed] a reasonably foreseeable risk" of "reputational injury" and other effects, which may have been hard to measure. Businesses would have also been required to "identify and weigh" the corresponding benefits against the potential for injury and produce the results upon request of the Attorney General.

Enforcement

SB 6281 vested exclusive enforcement authority with the state attorney general and explicitly precluded a private right of action. Violations of the bill would have been remediable by both injunctions and civil penalties of up to $7,500 per violation.

Facial Recognition

The bill also would have imposed special obligations on commercial entities that provide or utilize facial recognition services. This is in contrast to SB 6280, discussed below, which deals with use of facial recognition technology by state and local governmental entities. In particular, processors would have been required to "make available an application programming interface or other technical capability, chosen by the processor, to enable controllers or third parties to conduct legitimate, independent, and reasonable tests of those facial recognition services for accuracy and unfair performance differences across distinct subpopulations." Processors would have been also been required to contractually prohibit the use of facial recognition services by controllers for unlawful discrimination.

Additionally, controllers would have been required to "provide a conspicuous and contextually appropriate notice whenever a facial recognition service is deployed in a physical premise open to the public[.]" Controllers also would have been required 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," *unless* "for a security or safety purpose," which was subject to certain requirements. Controllers also would have been subject to a myriad of other requirements including periodic training, limitations on how facial recognition data could be used, and restrictions on when facial recognition data can be disclosed to law enforcement.

2. Why SB 6281 Failed and What to Expect Going Forward

SB 6281 passed the state Senate with overwhelming support. The House, however, passed a number of amendments, including one that would have established a private right of action for violations, and a conference committee was unable to reach agreement before the end of the legislative session. Senator Reuven Carlyle, the key Senate bill sponsor, said in a statement on March 12th that "[t]he impasse remains a question of enforcement," particularly over whether to include a private right of action. Senator Carlyle noted his view that "strong attorney general enforcement to identify patterns of abuse among companies and industries is the most responsible policy and a more effective model than the House proposal to allow direct individual legal action against companies."

The House hearings point to the debate over a private right of action being perhaps the most critical issue going forward. The House committee on Innovation, Technology & Economic Development ("ITED") released a bill report at the end of February that summarizes public testimony by stakeholders. The ITED bill report notes that some commenters expressed their belief that "the lack of private right of action in the bill eviscerates any meaningful notion of enforcement," while opponents of private rights of action argued that such a policy would "drive[] frivolous lawsuits and hurt[] innovation without adding privacy protections for consumers." This battleground is a familiar one: the debate over private rights of action was one of the issues that ultimately led to the collapse of SB 6281's precursor in 2019.

Businesses should take a close look at the requirements of SB 6281 and monitor developments closely in the next legislative session. If the issue of a private right of action can be resolved, Washington may enact a far-reaching privacy bill that would require substantial obligations on business, and which also differs in a

number of ways from the approach under California law. And other states considering privacy legislation may look toward the Washington model as well.

3. The Facial Recognition Bill

While SB 6281 failed, Washington did ultimately pass SB 6280, a privacy bill aimed at the use of facial recognition technology by state and local governmental entities. Its substantive requirements in this area are wide-ranging. In particular, the bill requires "[a] state or local government agency using or intending to develop, procure, or use a facial recognition service" to:

- File a "notice of intent" with a "legislative authority" (*g.*, city council);
- Procure an "accountability report"—a document that must include, *inter alia*, the name of the facial recognition vendor, a data management policy, measures taken to minimize inadvertent collection, data security measures, and much more—for the facial recognition service prior to developing, procuring, or using it;
- Allow for a "public review and comment period" of the accountability report with "at least three community consultation meetings;"
- "[C]learly communicat[e]" the accountability report to the public at least 90 days prior to putting it into operational use;
- Update the accountability report every two years;
- Amend the accountability report only through public notice and comment;
- Require vendors to disclose any complaints or report of bias;
- Ensure "meaningful human review" of any decisions made with the help of a facial recognition service that "produce legal effects" or "similarly significant effects concerning individuals;"
- Test the facial recognition service before putting it into operation;
- Require the facial recognition vendor to facilitate "legitimate, independent, and reasonable tests . . . for accuracy and unfair performance differences across distinct subpopulations."
- Develop a plan to mitigate any unfair performance differences across distinct subpopulations;
- Conduct periodic training for individuals that use the facial recognition service;
- Maintain records to facilitate "public reporting and auditing of compliance with the agency's facial recognition policies."

In addition to these requirements, the bill also imposes several obligations related to criminal justice. It requires state or local government agencies to "disclose their use of a facial recognition service on a criminal defendant to that defendant in a timely manner prior to trial." It precludes state or local government agencies from using facial recognition technology for ongoing surveillance, unless they have a warrant or court order, or "[e]xigent circumstances exist." It bars usage for a discriminatory purpose, "as the sole basis to establish probable cause in a criminal investigation," or to "identify an individual based on a sketch or other manually produced image." The bill also requires both state agencies who apply for warrants and judges who issue

warrants "for the use of a facial recognition service" to maintain detailed records of such application or issuance. Finally, the bill precludes government entities from "substantively manipulat[ing] an image for use in a facial recognition service in a manner not consistent with the facial recognition service provider's intended use and training."

All of these requirements contain a grandfathering provision exempting "facial recognition service[s] under contract as of" July 1, 2021, when the law would become effective. The bill now goes to the Governor for approval. Though it does not apply to all uses of facial recognition technology in the state, if approved it would impose significant limitations on how the technology can be used in practice. And in the future, the legislature may again take up commercial uses of facial recognition as it attempted to do in SB 6280.