As of March 12, 2020, the proposed Washington Privacy Act has foundered on enforcement rocks. The Senate did not agree with the House’s amendment that would have included a broad private right of action. The Senate’s version gave sole enforcement authority to the state Attorney General.

There are several states with pending legislation similar to this Act and the California Consumer Privacy Act, however given the impact of the COVID-19 pandemic, it remains to be seen whether these will advance.

Aristotle first suggested that “nature abhors a vacuum,” meaning that where there is a void, the universe seeks to fill it. Although there has been some movement in Congress towards comprehensive federal privacy legislation (see our
posts [here](#) and [here](#), states like California have taken up the gauntlet to fill the vacuum. We now have the [California Consumer Privacy Act (CCPA)](#) in force and expect to see other states take up similar laws this year.

In 2019, Washington State introduced the Washington Privacy Act (WPA), which passed in the Senate, but did not pass in the House during the 2019 legislative session. This month, a bipartisan group of legislators introduced an updated version of the WPA.

The WPA is more comprehensive than the CCPA, and borrows many concepts from the European Union’s landmark General Data Protection Regulation (GDPR). Similar to the CCPA and the GDPR, the WPA takes a holistic approach to privacy, recognizing privacy as a fundamental right and an essential element of individual freedom. This trend is in contrast to existing U.S. sectoral-based privacy laws that operate to recognize privacy rights only in certain contexts, such as health information, financial information, and information about children, to name a few.

If enacted, the WPA has the potential to surpass the CCPA to become the most comprehensive U.S. privacy law to date. Below is our summary of its key concepts.

**To Whom Would the WPA Apply?**

The WPA would apply to companies that conduct business in the State of Washington, or produce products or services targeted to Washington residents, and satisfy one or more of the following:

- Controls or processes personal data of 100,000 or more consumers; or
- Derives greater than 50% of gross revenue from the sale of personal data, and processes or controls personal data of 25,000 or more consumers.

**Important Definitions:**

- "Consumer" means a natural person who is a Washington resident acting only in an individual or household context. **It does not include a natural person acting in a commercial or employment context.**

- "Controller" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include deidentified data or publicly available information.

- "Processor" means a natural or legal person who processes personal data on behalf of a controller.

- "Sale," "sell," or "sold" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. "Sale" does not include the following: (i) The disclosure of personal data to a processor who processes the personal data on behalf of the controller; (ii) the disclosure of...
personal data to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer or otherwise in a manner that is consistent with a consumer’s reasonable expectations considering the context in which the consumer provided the personal data to the controller; (iii) the disclosure or transfer of personal data to an affiliate of the controller; or (iv) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller’s assets.

**Consumer Rights**

The WPA would give consumers the following rights with respect to their personal data:

- **Right of access**: Consumers would have the right to confirm whether or not a controller is processing their personal data, and the right to access such personal data.

- **Right to correction**: Consumers would have the right to correct their data.

- **Right to deletion**: Consumers would have the right to request that their data be deleted.

- **Right to data portability**: When exercising their right to access personal data, consumers would have the right to obtain personal data concerning them in a portable and, to the extent technically feasible, readily usable format.

- **Right to opt out**: Consumers would have the right to opt out of the processing of their personal data for purposes of targeted advertising, sale of personal data, or profiling in furtherance of decisions that produce legal or significant effects on the consumer.

**Controller Responsibilities**

The WPA would create the following controller responsibilities:

- **Transparency**
  
  - Controllers would be required to provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes: (i) the categories of personal data processed; (ii) the purposes for which the categories of personal data are processed; (iii) how and where consumers may exercise their rights; (iv) the categories of personal data that the controller shares with third parties; and (v) the categories of third parties with whom the controller shares personal data.

  - If a controller “sells” personal data or processes personal data for targeted advertising, it must clearly and conspicuously disclose such processing, and how a consumer may opt out.
• **Purpose Specification**
  - Personal data collection would be limited to what is reasonably necessary in relation to the specified and express purposes for which it is processed.

• **Data Minimization**
  - Personal data collection would be required to be adequate, relevant, and limited to what is reasonably necessary in relation to specified purpose.

• **Avoid Secondary Use**
  - The WPA would prohibit processing of personal data for purposes not reasonably necessary to or compatible with the specified purpose, unless the controller obtains the consumer’s consent.

• **Security**
  - Controllers would be required to establish, implement and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data.

• **Nondiscrimination**
  - Controllers would be prohibited from processing personal data in violation of antidiscrimination laws, and could not discriminate against consumers for exercising their rights under the WPA, including by denying goods/services, or providing a different quality of goods/services.

• **Sensitive Data**
  - The WPA would restrict processing of sensitive data without consumer consent.

• **Minors and Children**
  - The WPA would prohibit processing of personal data of a known child without consent of the child’s parent or legal guardian.

• **Non-waiver of Consumer Rights**
  - Under the WPA, any contract or agreement that waives or limits consumers’ WPA rights would be void and unenforceable.

**Processor Responsibilities**

The WPA would place the following responsibilities directly on data processors:

• Implement appropriate technical and organizational measures for fulfillment of controllers’ obligations to respond to consumer rights requests

• Breach notification requirements
• Reasonable security procedures and practices to protect personal data
• Confidentiality
• Provide controllers with the right to object to subcontractors; and
• Allow for controller audits

Processors also must have contracts in place with controllers that contain certain provisions regarding the processing of personal data. Those familiar with the GDPR will recognize that many of the WPA required provisions are similar to GDPR’s Article 28 data processing requirements.

Responding to Consumer Rights Requests

Under the WPA, controllers would be required to respond to consumer requests within 45 days of receipt (which may be extended by an additional 45 days if necessary).

Controllers would also be required establish an internal process for appeals, as well as a mechanism for consumers to easily submit a summary of their appeal and the outcome to the Attorney General.

**Note:** All information received by the Attorney General with respect to controller appeals would be made publicly available on the Attorney General’s website (with consumer personal data redacted).

Data Protection Assessments

Controllers would be required to conduct data protection assessments of each of their processing activities, and additional assessments whenever there is a change in processing that materially increases the risk to consumers. Such assessments must identify and weigh the benefits that may flow from the processing, against the potential risk to the rights of the consumer. If the risks outweigh the benefits and interests in certain circumstances, the controller may only engage in such processing with the consumer’s consent, unless an exemption applies.

The Attorney General would require controllers to disclose assessments upon request, and would evaluate the assessments for compliance with the WPA.

Liability For Third Party Processing

The WPA would not impose liability on controllers and processors for third party processing if the disclosure to such third party controller or processor complies with the WPA, provided that the disclosing controller or processor did not have knowledge that the third party intended to commit a violation.

Enforcement

The Attorney General would have exclusive authority to enforce the WPA, and could seek penalties of up to $7,500 per violation.
The WPA does not create a private right of action.

**Exemptions and Limitations on WPA Applicability**

Certain organizations and types of information would be exempt from the WPA:

- State and local government and municipal corporations;
- Certain information governed by other laws such as the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Family Educational Rights and Privacy Act, and the Children’s Online Privacy Protection Act;
- Employee information; and
- Certain de-identified or pseudonymous data

The WPA also contains several context-based exemptions, making clear, for example, that the WPA does not restrict a controller’s or a processor’s ability to: comply with laws or legal process, or cooperate with law enforcement investigations; prevent or identify certain wrongdoing; or use personal data for certain specified internal purposes.

**Facial Recognition**

The WPA would also regulate facial recognition services, placing a number of restrictions and obligations on facial recognition services providers, as well as controllers and processors of facial recognition data, including:

- Performance testing and biannual reviews;
- Safeguards against protected class discrimination;
- Consumer disclosures and required consent in certain cases;
- Required deletion of data after certain time periods; and
- Employee training

©1994-2020 Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. All Rights Reserved.