Brief Summary of 2SSB 6281
Senator Carlyle
An ACT Relating to the management and oversight of personal data

---

- Provides that this act shall be known as the Washington Privacy Act

- Provides findings that the people of Washington regard their privacy as a fundamental right and that Washington's Constitution explicitly provides the right to privacy

- Specifies that this act:
  - *Applies* to legal entities that conduct business or produce products targeted to Washington residents and:
    - Control or process personal data of more than 100,000 consumers during a calendar year; or
    - Derive 50 percent of gross revenue from the sale of personal data and process or control the personal data of over 25,000 consumers;
  - *Does not apply* to state agencies, local governments, or tribes; municipal corporations; personal data governed by certain state and federal regulations; and employment records

- Provides consumers with the following rights regarding their personal data:
  - *Access*: Confirmation if a controller is processing their data and access to that data
  - *Correction*: Correct inaccurate data
  - *Deletion*: Delete personal data
  - *Data Portability*: Obtain personal data in a portable format to transmit to another entity
  - *Opt-out*: Opt-out of the processing of personal data for the purposes of targeted advertising, the sale of personal data, and profiling in furtherance of decisions that produce legal effects

- Provides that a controller or processor is not required to take certain steps in order to comply with this act, such as identifying deidentified data or maintaining data in an identified form

- Requires controllers that use deidentified or pseudonymous data to exercise reasonable oversight

- Outlines controller responsibilities, including:
  - *Transparency*: Provide a privacy notice that meets certain requirements, including telling consumers how they can exercise their rights
  - *Purpose Specification*: Limit collection of data to what is required for a specified purpose
  - *Data Minimization*: Limit collection of data to what is relevant to a specified purpose
  - *Avoid Secondary Use*: Prohibit processing for purposes not compatible with a specified purpose
  - *Security*: Secure personal data from unauthorized acquisition
  - *Non-Discrimination*: Prohibit processing which violates state or federal law and discriminating against a consumer for exercising any of the consumer rights of this act
  - *Sensitive Data*: Obtain consumer consent in order to process sensitive data
  - *Nonwaiver of Consumer Rights*: Prohibit contract provisions that limit consumer rights

- Requires controllers to conduct a data protection assessment for specified processing activities involving personal data, including:
    - The processing for targeted advertising;
    - The sale of personal data;
    - Processing for purposes of profiling where reasonably foreseeable risks are present;
    - The processing of sensitive data; and
    - Any processing activities that present heightened risk of harm to consumers

- Authorizes the attorney general to request a data protection assessment relevant to an investigation and to evaluate it for compliance with responsibilities of this act and other laws

- Specifies limitations for when the obligations imposed on controllers or processors under this chapter do not restrict a controller or processor, i.e., complying with federal, state, or local laws

- Requires controllers or processors that process data pursuant to an exemption to demonstrate that the processing qualifies for an exemption and ensure that processing is limited and proportionate to that specified purpose

- Provides that any violation of this chapter does not serve as the basis for a private right of action under this act or any other law

- Authorizes the attorney general to bring an action and prescribes a penalty of not more than $7,500 for each violation

- Provides that this chapter preempts laws, ordinances, regulations, or the equivalent adopted by any local entity regarding the processing of personal data by a controller or processor

- Requires the attorney general to submit a report by July 1, 2022, evaluating the liability and enforcement provisions of this act and providing recommendations for any changes

- Provides a regulatory framework for the commercial use of facial recognition services by controllers and processors, including:
    - Third-party testing of the technology for accuracy and unfair performance
    - Testing of the service in operational conditions prior to deployment
    - Consumer consent prior to enrolling an image in a service used in a public space
    - Conspicuous notice where the service is deployed in a public space
    - Periodic training for all service operators

- Provides on effective date of July 31, 2021
    - July 31, 2024: Date of application for institutions of higher education and nonprofit corporations delayed three years