HB 567 Overview

Application

Bill covers personal data, defined as "data that can be reasonably linked to an identified or identifiable consumer."

- It also addresses sensitive data (biometrics, child data, consumer health data, data revealing race, gender identity, etc.)

The bill applies to a person that:

- Conducts business in the state; or
- Produces services or products that are targeted to residents of the state; and
    - Controlled or processed the personal data of at least 35,000 consumers (excluding solely for a payment transaction); or
    - Controlled or processed the persona data of at least 10,000 consumers and derived 20% of gross revenue from the sale of personal data.

Bill exempts several entities, as well as a number of specific types of data.

Consumer Rights

Bill grants consumers certain rights:

1. Right to confirm a controller is processing their personal data
2. Access that data
3. Correct the data
4. Require the controller to delete the data
5. Obtain a copy of the data
6. Obtain a list of categories of 3d parties to whom the controller has disclosed the personal data
7. Opt-out of the processing for:
    a. Targeted advertising
    b. The sale of personal data
    c. Profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.
8. Designate an authorized agent to opt-out of the processing in #7.

Exercising those rights

A controller:

1. Must establish a secure way for consumers to exercise their rights.
2. Shall respond to the request w/in 45 days. Can extend
3. Must notify the consumer w/in 15 days that they complied.
4. May decline. If they do, they shall inform the consumer and provide an appeal process.

Controllers

Controllers are the one who "determines the purpose and means of processing personal data." The bill puts guardrails on controllers' activities: data minimization, restrictions on collection and use of sensitive data, protecting data confidentiality, limits on the use of personal data

Details:

A. If a controller processes data

- They shall protect the confidentiality and security of the data
- Reduce risks of harm to the consumers relating to the collection, use or retention of the data
- Process the data to the extent it is reasonably necessary and proportionate to the purposes in the bill & is adequate, relevant & limited to what is necessary.

B. Responsibilities

A controller may not:

1. Collect personal data for the sole purpose of content personalization or marketing, unless they have the consumer's consent.
2. Collect, process, or share sensitive data concerning a consumer (except where strictly necessary to provide or maintain a specific product or service requested by the consumer, and only with the consumer's consent).
3. Sell sensitive data
4. Process personal data in violation of anti-discrimination laws
5. Process personal data for purposes of targeted advertising or sell the consumer's personal data, if controller knows or has reason to know the consumer is between 13-18.
6. Discriminate against a consumer for exercising their rights under this title.
7. Collect, process, or transfer personal data in a way that discriminates or makes unavailable the equal enjoyment of goods (Civil Rights lang. from bi-partisan federal bill)
8. Process personal data for a purpose that is not reasonably necessary to or compatible with the disclosed purposes for which the data is processed (unless consumer consents).

A controller shall:

1. Limit the collection of personal data to what is reasonably necessary and proportionate to provide or maintain a service requested by a consumer.
2. Establish reasonable security practices to protect the data
3. Provide a reasonable mechanism for a consumer to revoke consent.
4. Stop processing data within 15 days of a consent revocation.
5. Provide a clear privacy notice that includes:
    a. Categories of personal data processed, including sensitive data
    b. Purpose for processing the data
    c. How a consumer may exercise their rights
    d. Categories of 3d parties with which the controller shares data, with sufficient detail so the consumer understands what they are and how they may process the data
    e. Categories of data shared with 3d parties
    f. Active email address to contact the controller

C. **Other**

Nothing in this bill:

1. Requires a controller to provide a product or service that requires data they don't collect
2. Prohibits a controller from offering different levels of service if the offering is in connection with a loyalty program.

Processors

A processor is "a person that processes personal data on behalf of a controller."

Processors & controllers must enter a contract that includes:

- Instructions for processing the data
- Nature and purpose of processing
- Type of data subject to processing
- Duration of processing
- Duty of confidentiality
- Issues of retention/return/deletion of data

Processors:

1. Help controllers comply with the Act
2. May engage subcontractors with controller's consent

Controller v. processor? A processor

- is limited in processing of specific data per controller's instruction
- can be deemed a controller if they
    - fail to adhere to instructions
    - determine purposes and means of processing data

"Processing Activities that Present a Heightened Risk of Harm" & Data Assessments

This section sets out requirements for processing activities that 'present a heightened risk of harm.' Those are defined as:

1. the processing of personal data for targeted advertising
2. the sale of personal data
3. the processing of sensitive data
4. processing of personal data for the purposes of profiling, which risks
    a. unfair, abusive or deceptive treatment
    b. having an unlawful disparate impact
    c. financial, physical, or reputational injury
    d. physical or other intrusion into private affairs
    e. other substantial injury

For each activity in #4, a controller must conduct a data protection assessment. This assessment shall:

1. identify and weigh the benefits to the controller, the consumer, & the public against the risks to the consumer (as mitigated by any safeguards the controller employs) and the necessity of processing in relation to the stated purpose of the processing.

2. Include various factors, such as
    a. The use of de-identified data
    b. Consumer expectations
    c. Context
    d. Relationship between controller and consumer
3. Be made available to the OAG Div. of Consumer Protection where relevant to an investigation.

Misc.

These pages lay out a series of things the tech industry negotiated for in other states' bills. For example, they do not have to:

- Maintain data in an identifiable form
- Collect any data to authenticate a consumer request
- Comply with a request if they can't associate the request with the data

The bill doesn't restrict controllers or processors from a litany of actions, including complying with laws, subpoenas, cooperate with law enforcement, establish a defense to a claim, provide a product specifically requested, perform under a contract, protect life or physical safety, prevent/detect fraud, assist another with obligations under this bill, effectuate a recall, identify & repair technical errors, perform internal operations.

Enforcement

By the Office of the Attorney General
No Private Right of Action
Violation is an unfair, abusive or deceptive trade practice
Other remedies at law available to consumers