
**Innovation, Technology & Economic
Development Committee**

HB 2046

Brief Description: Increasing consumer data transparency.

Sponsors: Representatives Kloba, Tarleton, Smith, Hudgins, Slatter, Frame, Stanford, Valdez and Pollet.

Brief Summary of Bill

- Requires processors of personal data to provide consumers with a privacy notice about their privacy and security practices.
- Requires processors that sell or otherwise monetize personal data to inform data subjects of, and provide access to a record of, each such agreement or transaction.
- Makes violations of the notice and information requirements enforceable under the Consumer Protection Act and subject to both civil penalties and statutory damages.

Hearing Date: 2/20/19

Staff: Yelena Baker (786-7301).

Background:

Personal information and privacy interests are protected under various provisions of state law. The Washington State Constitution provides that no person shall be disturbed in his private affairs without authority of law. The Public Records Act protects a person's right to privacy under certain circumstances if disclosure of personal information would be highly offensive and is not of legitimate concern to the public.

The Consumer Protection Act (CPA) prohibits unfair methods of competition and unfair or deceptive practices in the conduct of any trade or commerce. The Attorney General may investigate and prosecute claims under the CPA on behalf of the state or individuals in the state.

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

A person or entity found to have violated the CPA is subject to treble damages and attorney's fees.

Summary of Bill:

"Data subject" means an identified or identifiable natural person who is a Washington resident.

"Personal data" means information that identifies, relates to, describes, or could reasonably be linked, directly or indirectly, with a particular data subject, and includes biometric information, geolocation data, and commercial information such as a record of products and services purchased or consumed.

"Processor" means a natural or legal person, public authority, agency, or other body that processes personal data. If a processor does not control the purposes or means of the processing of personal data, the entity with such control is also considered a processor. "Process" means any operation or set of operations that is performed on personal data or sets of personal data, whether or not by automated means.

Specific notice requirements apply to processors established in Washington; the same requirements apply to processors not established in Washington if the processing activities are related to:

- the offering of goods and services to data subjects;
- the monitoring of data subjects' behavior if that behavior takes place in Washington.

A processor must provide data subjects with a timely and conspicuous notice about the processor's privacy and security practices, including a detailed description of the personal data being processed, the sources of data, the purposes for which personal data is used, and the persons or categories of persons to which the processor discloses or allows access to the personal data. The notice must also provide data subjects with a meaningful opportunity to access their personal data and grant, refuse, or revoke consent for the processing of personal data.

A processor that sells or otherwise monetizes personal data must inform data subjects of each agreement or transaction for the sale or monetization of the data subject's personal data and provide data subjects reasonable access to a record of all such agreements. "Monetize" means share, leverage, process or allow processing of personal data to generate economic benefits, including market share and market value gains. Upon the data subject's request, the processor must also provide the specific categories of personal data sold or monetized.

The notice requirements do not apply to publicly available information, employment-related information when processed for employment-related purposes only, and data sets regulated by the federal Health Insurance Portability and Accountability Act (HIPPA), the Gramm-Leach-Bliley Act, and the Fair Credit Reporting Act.

Violations of these provisions are enforceable by the Attorney General under the Consumer Protection Act and subject to civil penalties of up to \$15,000 for each violation, with presumed restitution of at least \$1,000 per affected consumer. A data subject prevailing in an action for violations of these provisions does not need to prove actual damages and may recover statutory damages of up to \$15,000 for each violation.

Appropriation: None.

Fiscal Note: Requested on February 18, 2019.

Effective Date: The bill takes effect 90 days after adjournment of the session in which the bill is passed.