Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Innovation, Technology & Economic Development Committee

HB 1503

Brief Description: Concerning registration and consumer protection obligations of data brokers.

Sponsors: Representatives Smith, Hudgins and Stanford.

Brief Summary of Bill

- Requires data brokers to register annually, disclose certain information regarding their practices, and to implement a comprehensive information security program to protect personally identifiable information.
- Prohibits acquisition of brokered personal information through fraudulent means or acquisition of brokered personal information for the purpose of stalking, committing a fraud or engaging in unlawful discrimination.
- Directs the Attorney General and the Chief Privacy Officer to submit certain reports to the Legislature.

Hearing Date: 2/5/19

Staff: Yelena Baker (786-7301).

Background:

According to the Federal Trade Commission, companies known as "data brokers" collect personal information from consumers and sell or share it with others. Data brokers collect this information from a wide variety of commercial and government sources, and use both raw and inferred data about individuals to develop and market products, verify identities, and defect fraud. Because these companies generally never interact directly with consumers, consumers are often unaware of their existence, practices, and use of collected personal information.

The state Consumer Protection Act (CPA) prohibits unfair or deceptive acts or practices in trade or commerce. A private person or the Attorney General may bring a civil action to enforce the

---

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.

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

Summary of Bill:

Definitions.
"Brokered personal information" means one or more of the computerized data elements about a consumer, categorized or organized for dissemination to third parties, and includes name, address, date and place of birth, and other information that would allow a reasonable person to identify the consumer with reasonable certainty.

"Data broker" means a business that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.

Businesses that provide publicly available information via real-time or near real-time alert services for health or safety purposes and collect and sell brokered personal information incidental to those activities are not data brokers.

Requirements for data brokers.
Data brokers are required to register annually with the Chief Privacy Officer, pay a $250 registration fee, and provide certain information regarding their practices related to the collection, storage or sale of brokered personal data, including whether the data brokers permit consumers to opt out from data collection or sale of personal information.

Data brokers are required to develop, implement, and maintain a comprehensive information security program that contains appropriate administrative, technical, and physical safeguards to protect personally identifiable information. The security program must include certain features, such as identification and assessment of reasonably foreseeable risks, ongoing employee training, supervision of service providers, and regular monitoring to ensure proper operation. The security program must also include specified computer system security elements, including secure use authentication protocols, encryption of all files containing personally identifiable information, and reasonable monitoring of systems for unauthorized access or use.

Brokered personal information may not be acquired through fraudulent means or for the purpose of stalking, committing a fraud or engaging in unlawful discrimination.

Enforcement.
Violations of these provisions are enforceable solely by the Attorney General under the Consumer Protection Act.

Failure to register and to provide required information is subject to a fine of up to $10,000 a year and other penalties imposed by law.

Reports to the Legislature.
The Attorney General must review and consider additional legislative approaches to protecting the data privacy of Washington consumers, and to report its findings to the economic development committees of the Legislature by January 1, 2020.

The Attorney General and the Chief Privacy Officer must submit a preliminary report concerning the implementation of this bill to the economic development committees of the Legislature by July 1, 2021.

Appropriation: None.

Fiscal Note: Available.

Effective Date: The bill takes effect January 1, 2020, except Section 6, which relates to reports requirements and which takes effect 90 days after adjournment of the session in which the bill is passed.