HOUSE BILL REPORT
HB 1503

As Reported by House Committee On:
Innovation, Technology & Economic Development

Title: An act relating to registration and consumer protection obligations of data brokers.

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

Sponsors: Representatives Smith, Hudgins and Stanford.

Brief History:
Committee Activity:
Innovation, Technology & Economic Development: 2/5/19, 2/13/19 [DPS].

Brief Summary of Substitute 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.
- Authorizes the Chief Privacy Officer to coordinate with the Department of Revenue for the purpose of collecting data brokers' annual registration fees.
- Prohibits acquisition of brokered personal information through fraudulent means or 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.

HOUSE COMMITTEE ON INNOVATION, TECHNOLOGY & ECONOMIC DEVELOPMENT

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 6 members: Representatives Hudgins, Chair; Kloba, Vice Chair; Smith, Ranking Minority Member; Boehnke, Assistant Ranking Minority Member; Slatter and Tarleton.

Minority Report: Without recommendation. Signed by 1 member: Representative Van Werven.

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.

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 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 Substitute Bill:

Definitions.
"Brokered personal information" means one or more 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 the 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 against 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.

Substitute Bill Compared to Original Bill:

The substitute bill: (1) excludes from the definition of "data broker" businesses that provide 411 directory assistance or directory information services on behalf of, or as a function of, a telecommunications carrier; (2) specifies that "breach of the security of the system" has the same meaning as in the data breach notification provisions (RCW 19.255.010); (3) adds a definition of "Chief Privacy Officer"; and (4) authorizes the Chief Privacy Officer to coordinate with the Department of Revenue for the purpose of collecting data brokers' annual registration fees.

Appropriation: None.

Fiscal Note: Available.

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

Staff Summary of Public Testimony:

(In support) This data broker registration bill largely mirrors what has already been done in Vermont, with some modifications based on differences in state government organization and in the data breach laws. Data brokers are companies that an individual has no direct relationship with, but are companies that acquire thousands of data points about individuals,

creating a profile, and monetizing that information in some way. The concerns about the lack of transparency into this industry sector have been repeatedly brought up in testimony before Congress. This bill is a way to ask some questions in order to begin to understand the data broker industry. Credit bureaus are subject to certain federal laws. More than 145 million Americans were impacted by the Equifax data breach, and much of the collected information was not covered by federal law because a large portion of Equifax business was not credit reporting but a data broker business. When one looks at what is being collected, it is truly troubling and concerning. According to a report from the Vermont Attorney General, some of the collected data include information about rape survivors, addresses of domestic violence shelters, state troopers' home addresses, and information about people who suffer from various diseases. People have no say in the profile that is created about them or whether it is accurate. This bill opens a window to empower each Washingtonian to have more control over data privacy.

(Opposed) The references to security breaches or data breaches overlap with Washington's data breach notification law. The activities of the consumer reporting agencies, or credit bureaus, should be exempt. The data breach obligations are duplicative and redundant, considering the existing Washington state data breach laws. The substitute version of the bill appears to address this issue.

(Other) This bill was not contemplated in the Governor's budget. The policy priorities established here are extremely important and the committee should take appropriate action. Privacy professionals have heard from all over the state that Washingtonians value their privacy and the constitutional protection for the right to be undisturbed in their private affairs. Washingtonians are very concerned about third-party data sales and how data brokerage affects them and their families. This is an important issue and a moderate, well-thought out bill. The implementation should be relatively simple.

Persons Testifying: (In support) Representative Smith, prime sponsor.

(Opposed) Cliff Webster, Consumer Data Industry Association; and Tom McBride, CompTIA.

(Other) Will Saunders, Office of Privacy and Data Protection.

Persons Signed In To Testify But Not Testifying: None.