HOUSE BILL REPORT
HB 1493

As Reported by House Committee On:
Technology & Economic Development

Title: An act relating to biometric identifiers.

Brief Description: Concerning biometric identifiers.

Sponsors: Representatives Morris, Harmsworth, Smith, Tarleton and Stanford.

Brief History:
Committee Activity:
Technology & Economic Development: 1/31/17, 2/14/17 [DPS].

Brief Summary of Substitute Bill

- Prohibits a person from enrolling a biometric identifier in a database for a commercial purpose without notice, consent, or a way to prevent subsequent use.
- Prohibits selling, leasing, or disclosing a biometric identifier for a commercial purpose unless consent is obtained or certain criteria are met.
- Establishes requirements regarding biometric identifier retention and access.
- Makes a legislative finding relating to the Consumer Protection Act, RCW 19.86.

HOUSE COMMITTEE ON TECHNOLOGY & ECONOMIC DEVELOPMENT

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 14 members: Representatives Morris, Chair; Kloba, Vice Chair; Tarleton, Vice Chair; Smith, Ranking Minority Member; DeBolt, Assistant Ranking Minority Member; Doglio, Harmsworth, Hudgins, McDonald, Santos, Slatter, Steele, Wylie and Young.

Minority Report: Without recommendation. Signed by 2 members: Representatives Fey and Nealey.

Minority Report: Do not pass. Signed by 1 member: Representative Manweller.

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: Lily Smith (786-7175).

Background:

Biometrics.

The terms "biometric data," "biometric information," or "biometric identifier" variously refer to measurable biological or behavioral characteristics unique to an individual. Biometrics may be used for identification and authentication purposes, such as unlocking a device or authorizing a payment. They may also be used to gather personal characteristics for customizing services or information, such as in advertising.

Federal Regulation.

There is no federal law that specifically regulates the collection or use of biometric data for commercial purposes. The Federal Trade Commission (FTC) has the authority to enforce privacy and data security through the regulation of unfair or deceptive acts or practices in or affecting commerce, and several federal laws regulate the use of personally identifiable information. The Gramm-Leach-Bliley Act requires financial institutions to explain how they share information, and gives consumers the right to place some limits on how their information is shared.

In 2012 the FTC released recommended best practices for companies that use facial recognition technologies. The three major principles of the best practices are:

1. privacy by design;
2. simplified choice; and
3. greater transparency.

State Regulation.

No Washington law comprehensively regulates the collection or use of a person's biometric data for commercial purposes.

State Security Breach Laws.

Parallel security breach laws apply to agencies and to any person or business (chapter 19.255 RCW and chapter 42.56 RCW). These laws require any person, business, or agency to notify possibly affected persons when security is breached and personal information is (or is reasonably believed to have been) acquired by an unauthorized person. Disclosure is not required if a breach is not reasonably likely to subject customers to a risk of harm. A consumer injured by a violation of these laws may bring a civil action to recover damages and seek an injunction. The Attorney General may also bring an action for enforcement against a person, business, or agency.

State Consumer Protection Act.

Under Washington's Consumer Protection Act (CPA), "unfair or deceptive acts or practices" in trade or commerce are unlawful. The CPA provides that any person who is injured in his

or her business or property through such practices may bring a civil action to recover actual damages sustained and costs of the suit, including reasonable attorney's fees. Treble damages may also be awarded in the court's discretion, provided the damage award does not exceed $25,000. The Attorney General may also bring an action under the CPA in order to restrain and prevent unfair and deceptive acts and practices.

Summary of Substitute Bill:

A person may not enroll a biometric identifier in a database for a commercial purpose, without providing notice, obtaining consent, or providing a mechanism to prevent subsequent use. A biometric identifier enrolled or obtained for a commercial purpose may not be used in a way inconsistent with the original terms under which it was provided, unless new consent is obtained.

The sale, lease, or disclosure of a biometric identifier for a commercial purpose, without the individual's consent, is prohibited unless it is:

- consistent with the database enrollment, protection, and retention requirements;
- necessary in providing a product or service requested by the individual;
- necessary in completing a financial transaction that the individual requested or authorized;
- expressly required or authorized under a federal or state statute;
- made to facilitate a law enforcement response to an ongoing incident; or
- made to prepare for litigation or for the purpose of judicial process.

A person in possession of biometric identifiers enrolled for a commercial purpose must guard against unauthorized access and adhere to retention limitations. The limitations on disclosure and retention do not apply if the biometric identifiers have been unenrolled.

Violations may be enforced by the Attorney General under the CPA.

"Biometric identifier" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas or irises, or other unique biological patterns or characteristics that are used to identify a specific individual.

"Biometric system" means an automated identification system capable of capturing, processing, and storing a biometric identifier, comparing the biometric identifier to one or more references, and matching the biometric identifier to a specific individual.

"Capture" means the process of collecting a biometric identifier from an individual.

"Commercial purpose" means a purpose in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing of goods or services when such goods or services are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier. It does not include a security purpose.

Substitute Bill Compared to Original Bill:

The provisions relating to notice and consent are modified as follows:

- A person may provide notice, obtain consent, or provide a way to prevent subsequent use before enrolling a biometric identifier, instead of needing to both provide notice and obtain consent.
- The notice provided must be readily available to affected individuals, instead of being clear, conspicuous, and given through a procedure reasonably designed to be prominent, timely, relevant, and easily accessible.
- The sale, lease, or disclosure of a biometric identifier is permitted if consent is obtained.

The prohibitions on enrolling a biometric identifier in a database without notice or consent, and subsequent use and disclosure, are limited to instances that involve a commercial purpose. The definition of "commercial purpose" is narrowed to when furthering a sale or disclosure to a third party. A person must knowingly possess a biometric identifier for the retention and protection provisions to apply.

Specific exclusions are made:

- for activities subject to the federal Health Insurance Privacy and Portability Act of 1996; and
- for the collection, capture, enrollment or storage of a biometric identifier for a security purpose.

A violation under the CPA is to limited to enforcement by the Attorney General.

The definition of "security purpose" is broadened to include other purposes in furtherance of protecting the security or integrity of software, accounts, applications, online services, or any person.

"Unique biological patterns" are added to the definition of biometric identifier.

A number of other minor and technical revisions are included.

Appropriation: None.

Fiscal Note: Available.

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

Staff Summary of Public Testimony:

(In support) This is a bipartisan effort to protect data that is part of our technology culture, while still allowing for innovation. Biometrics are unique in that they are sensitive and personal, and a person cannot be issued new ones. This bill would protect the data as it becomes personally identifiable information.

(Opposed) Biometrics are important for a number of security and other purposes. The use of the data may be restricted, but the collection should not be. Collection by itself does not cause harm. Protective laws already exist. Data should be protected only when it specifically identifies an individual. Do not support a private right of action. Definitions need to be clarified. It should be clear that collection by law enforcement does not constitute a commercial purpose, and video surveillance and photos should be exempted. This is a new industry and regulation should proceed cautiously.

Persons Testifying: (In support) Representative Morris, prime sponsor; and Representative Harmsworth.

(Opposed) Carolyn Logue, Washington Retail Association; Jim Justin, Washington Technology Industry Association; Bob Battles, Association of Washington Business; James McMahan, Washington Association of Sheriffs and Police Chiefs; and Tom McBride, Computing Technology Industry Association.

Persons Signed In To Testify But Not Testifying: None.