SENATE BILL REPORT
ESHB 1493

As Passed Senate, April 11, 2017

Title: An act relating to biometric identifiers.

Brief Description: Concerning biometric identifiers.

Sponsors: House Committee on Technology & Economic Development (originally sponsored by Representatives Morris, Harmsworth, Smith, Tarleton and Stanford).

Brief History: Passed House: 3/02/17, 81-17.
Committee Activity: Law & Justice: 3/14/17, 3/28/17 [DP, DNP, w/oRec].
Floor Activity:
Passed Senate: 4/11/17, 37-12.

Brief Summary of 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.

SENATE COMMITTEE ON LAW & JUSTICE

Majority Report: Do pass.
Signed by Senators Padden, Chair; O'Ban, Vice Chair; Angel and Wilson.

Minority Report: Do not pass.
Signed by Senators Pedersen, Ranking Minority Member; Darneille.

Minority Report: That it be referred without recommendation.
Signed by Senator Frockt.

Staff: Aldo Melchiori (786-7439)

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.

Background: 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.

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. 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. 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.

No Washington law comprehensively regulates the collection or use of a person's biometric data for commercial purposes. Parallel state 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 without authorization. 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 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.

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 their 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 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 or disclosed in a way inconsistent with the original terms under which it was provided, unless new consent is obtained.

A biometric identifier is 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.

A commercial purpose is 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 or law enforcement purpose.

To enroll means to capture a biometric identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual.

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;
- is made in good faith in response to a request by a law enforcement officer in 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 solely by the Attorney General under the CPA.

The provisions do not apply to financial institutions or affiliates subject to the Gramm-Leach-Bliley Act of 1999 or the federal Health Insurance Privacy and Portability Act of 1996.

Appropriation: None.

Fiscal Note: Available.

Creates Committee/Commission/Task Force that includes Legislative members: No.

Effective Date: Ninety days after adjournment of session in which bill is passed.

Staff Summary of Public Testimony: PRO: This is greatly improved over past legislative efforts. The bill does not regulate information used for identification purposes when making transactions. People always have a proprietary interest in their biometric information. The bill accounts for developing technology while limiting commercial use. It is important to have an open ended definition to account for future technological development.

CON: We need to move slowly and get this right. Policy should not get ahead of technology. These provisions may cause increased litigation. Some in the technology industry are neutral on the bill, but none support it. The term "biological patterns or characteristics" as used in the definition of biometric identifier does not provide clear guidance and is ambiguous. The bill should provide that the biometric identifier was collected from an individual in person.

Persons Testifying: PRO: Representative Morris, Prime Sponsor.

CON: Tom McBride, CompTIA; Joanie Deutsch, TechNet; Bob Battles, AWB.

Persons Signed In To Testify But Not Testifying: No one.