
**Technology & Economic Development
Committee**

HB 1493

Brief Description: Concerning biometric identifiers.

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

Brief Summary of Bill

- Prohibits a person from identifying an individual by enrolling a biometric identifier in a database without notice and consent.
- Prohibits selling, leasing, or disclosing a biometric identifier for a commercial purpose unless 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.

Hearing Date: 1/31/17

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.

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.

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 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 (GLBA) 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 Bill:

A person may not create identification of an individual by enrolling a biometric identifier in a database, without providing clear and conspicuous notice and obtaining the individual's consent. A person may not use a biometric identifier in a way inconsistent with the original terms of notice and consent, unless new consent is obtained.

The sale, lease, or disclosure of a biometric identifier for a commercial purpose is prohibited unless it is:

- consistent with specified notice, consent, 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 anonymized.

A legislative finding is included that the practices covered under this section are matters vitally affecting the public interest for the purpose of applying the Consumer Protection Act, and a material violation is not reasonable, or is an unfair or deceptive act.

"Biometric identifier" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voice, eye retina or iris, or other unique biological characteristic, which is used by the person or licensee to uniquely authenticate an individual's identity when the individual accesses a system or account.

"Biometric system" means an automated system capable of capturing a biometric sample from an individual, extracting and processing biometric data from that sample, storing the extracted information in a database, comparing the biometric data with data contained in one or more references, determining whether the biometric data matches the reference, and indicating whether or not an identification has been achieved.

"Capture" means the process of using a sensor to collect a biometric sample and related contextual data from a scene or an individual, or both, with or without the individual's knowledge.

Appropriation: None.

Fiscal Note: Available.

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