

HOUSE BILL REPORT

HB 1094

As Reported by House Committee On:
Technology & Economic Development

Title: An act relating to biometric identifiers.

Brief Description: Concerning biometric identifiers.

Sponsors: Representative Morris.

Brief History:

Committee Activity:

Technology & Economic Development: 1/21/15, 2/5/15 [DPS].

Brief Summary of Substitute Bill

- Defines biometric identifiers.
- Identifies when biometric identifiers may be captured or disclosed for a commercial purpose.
- Provides retention and storage requirements for biometric identifiers.
- Modifies who may recover costs and fees under the Consumer Protection Act in an action brought by the Attorney General.

HOUSE COMMITTEE ON TECHNOLOGY & ECONOMIC DEVELOPMENT

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 12 members: Representatives Morris, Chair; Tarleton, Vice Chair; Smith, Ranking Minority Member; DeBolt, Assistant Ranking Minority Member; Fey, Harmsworth, Hudgins, Nealey, Ryu, Santos, Wylie and Young.

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

Staff: Kirsten Lee (786-7133).

Background:

Federal Privacy Laws.

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.

Under both federal and state constitutional rights, an individual has a right to privacy, which includes an individual interest in avoiding disclosure of personal matters.

In the United States, an all-encompassing data privacy law does not exist. The Privacy Act of 1974 (Act) provides general protections for the collection, use, maintenance, and dissemination of personal identifiable information (PII) processed and held by the Federal Government. However, the Act does not apply to states, local governments, and the private sector, and does not provide specific protections for different types of data. Instead, individual sector-specific privacy laws are applied related to areas such as financial services, communications, and healthcare.

Similarly, biometrics are not currently protected by any specific federal law. Instead various general privacy laws apply both at the federal and state levels to PII, which include biometric data within the same sector specific laws. In more recent years, states have adopted biometric specific privacy laws.

Biometric specific state laws define biometrics, an area of PII, as specific biological, genetic and physical characteristics. These characteristics include, but are not limited to, finger prints, palm prints, hand geometry, iris scans, retina scans, eye vein scans, and voiceprint scans.

Washington state does not have a biometric specific privacy law.

Consumer Protection Act.

The Washington Consumer Protection Act (CPA) declares that unfair and deceptive practices in trade or commerce are illegal. The CPA allows a person injured by an unfair or deceptive practice to bring a private cause for damages. The Office of the Attorney General may investigate and prosecute claims under the CPA on behalf of the state or individuals in the state.

Under the CPA, "person" includes natural persons, corporations, trusts, unincorporated associations, and partnerships.

Summary of Substitute Bill:

This bill pertains to commercial use of biometric identifiers.

Definitions.

"Biometric Identifier" is defined in two ways. Both definitions refer to biological, behavioral, or both characteristics. Characteristics that uniquely identify an individual, such as fingerprint, DNA, hand geometry, palm print and iris scan enable automatic recognition and are considered biometric identifiers. Other less sensitive characteristics, including facial imaging, voice, and gait, are considered biometric identifiers if used for a specific automated identification purpose.

Collection and Disclosure.

Capture and disclosure of biometric identifiers for commercial purposes are confined to specific instances. Capture of an individual's biometric identifier is prohibited unless the individual:

- is informed before the capture; or
- gives consent.

If a person legally possesses a biometric identifier of an individual for commercial purposes, they are prohibited from selling, leasing, or otherwise disclosing the biometric identifier, unless:

- the individual consents to disclosure for identification purposes in the event of the individual's death or disappearance or otherwise consents to the disclosure of third parties;
- the person discloses the biometric data to a service provider or other third party as necessary to effect, administer or enforce, or complete a financial transaction that the individual requested, initiated, or authorized;
- disclosure is required or permitted by federal or state statute; or
- disclosure is made by or to law enforcement for a law enforcement purpose in response to a warrant.

Storage.

Storage, transmission and protection from disclosure of biometric identifiers must be done in a manner that uses reasonable care (same as or more protective than industry standards).

Retention.

Biometric identifiers must be retained no longer than is legally permissible as required by law or rule, particularly as necessary to protect against or prevent fraud, criminal activity, claims, or liability. Specific provisions are provided for contractual and employment relationships. In a contractual relationship, the purpose for collecting the biometric identifier expires upon the latter of termination of a continuous contractual relationship, after the time period necessary to carry out the terms of the contract, or as long as is permitted or required by law. In an employment relationship, the purpose for collecting the biometric identifier expires upon termination of the relationship.

Consumer Protection Act.

The CPA applies. When the prevailing party of an action, brought by the Attorney General under the CPA, is the Attorney General, costs and reasonable attorneys' fees may only be awarded to the Attorney General and not the defendant.

Substitute Bill Compared to Original Bill:

The substitute bill: (1) allows a person who legally possesses a biometric identifier to sell, lease, or disclose the biometric identifier(s) to third parties with an individual's consent; (2) allows a person who legally possesses an individual's biometric identifier to sell, lease or disclose the biometric identifier(s) to a service provider or other third party for the purpose of completing a financial transaction; (3) changes the standard for biometric retention from legally necessary to legally permissible and includes requirements specific to protecting and preventing actual or potential fraud, criminal activity, or claims or liability; (4) allows for retention of a biometric identifier beyond the end of a continuous contractual relationship

when collected for a contractual purpose by adding that the purpose may extend for as long as necessary to carry out the terms of a contract or for as long as permitted or required by law; (5) changes the definition of a biometric identifier to mean, characteristics that uniquely identify and enable automated recognition, instead of inherently sensitive and enables automated recognition; and (6) changes the definition of less sensitive biometric identifiers to require that the identifier be used specifically for automated identification purposes, instead of identification purpose to be considered a biometric identifier.

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) The specific concept of legislating in this area is to provide rules for deployment of newer technology. The idea is to determine what is the proper deployment standards for biometric identifiers and giving a consumer some control over their personal identifiable information. This gives the consumer control over what relationships they join and how that information is disseminated. Anyone should be able to use this technology if there is a willing relationship. The purpose of the bill, is to try to stop surreptitious collection of biometric information. The bill is establishing the propriety of the relationship and gives both parties, the owner deploying technology and consumer, certain rights in how the information is sold to someone else. There is some concern from law enforcement, but the bill is not effecting the normal practice of using video tape surveillance and providing those tapes, such as in a shoplifting case.

(With concerns) If a commercial entity wants to provide information such as video, palm prints, or iris scan without having to get a warrant, then they should be able to.

(Opposed) None.

Persons Testifying: (In support) Representative Morris, Prime Sponsor.

(With concerns) James McMahan, Washington Association of Sheriffs and Police Chiefs; and Mark Johnson, Washington Retail Association.

Persons Signed In To Testify But Not Testifying: None.