

SENATE BILL REPORT

ESHB 1094

As of March 24, 2015

Title: An act relating to biometric identifiers.

Brief Description: Concerning biometric identifiers.

Sponsors: House Committee on Technology & Economic Development (originally sponsored by Representative Morris).

Brief History: Passed House: 3/04/15, 91-6.

Committee Activity: Law & Justice: 3/23/15.

SENATE COMMITTEE ON LAW & JUSTICE

Staff: Aldo Melchiori (786-7439)

Background: Personal Identifiable Information. The Privacy Act of 1974, 5 U.S.C. § 552a (2006) provides general protections for the collection, use, maintenance, and dissemination of personal identifiable information (PII) processed and held by the federal executive branch agencies. However, the act does not apply to states, local governments, or 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. Biometric data are not currently protected by any specific federal law. Instead various general privacy laws apply to PII, both at the federal and state levels, which include biometric data within the same sector specific laws. Washington does not have a biometric-specific privacy law.

Consumer Protection Act (CPA). The 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 of action 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.

Summary of Bill: Capture and Collection. The capture 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; and
- gives consent.

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.

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

A biometric identifier captured for a noncommercial purpose may not be used for a commercial purpose at a later date without an individual's consent. When consent is provided for commercial use of a biometric identifier that was initially captured for a noncommercial purpose, consent requires an individual to actively opt in.

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

Retention. Biometric identifiers must be retained no longer than is legally permissible by law or rule, 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.

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. Video surveillance and photographs are not considered biometric identifiers.

Consent means an authorization by an individual, given after the individual has received clear and conspicuous notice in writing of the purposes for which the biometric identifier may be disclosed. If an individual consents to disclosure of their biometric identifier to law enforcement without a warrant, consent must be made separate from any other consent provided.

CPA. A violation of the requirements is considered an unfair or deceptive act in trade or commerce and an unfair method of competition for the purposes of applying the CPA.

Appropriation: None.

Fiscal Note: Available.

Committee/Commission/Task Force Created: No.

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

Staff Summary of Public Testimony: PRO: We need to make the biometric identifier rules clear. Ownership of biometric identifiers should remain in the hands of consumers. People should have control over how their biometrics are used. Businesses are free to use biometric identification for legitimate purposes. Consumers should be able to recover damages when biometric identifiers are misused. The bill allows for the development of new technology while protecting consumers. The opt-in provision prevents the hidden use of biometric identifiers.

CON: The definition of biometric identifiers is too broad. The use of data should be addressed instead of the use of technology. A federal law regarding the issue would be better than a patchwork of state laws. Innocent business owners may get swept into litigation and liability for damages. The bill includes some behavioral identifiers, but they are not defined clearly. Nearly all digital content includes some biological or behavioral identifier. The security standards should be consistent with the Federal Trade Commission standards.

OTHER: Biometrics can make identification more secure and help eliminate financial fraud. Care should be taken to not prohibit the beneficial use of biometrics.

Persons Testifying: PRO: Representative Morris; prime sponsor; Representative Harmsworth.

CON: Tom McBride, Tech America; Joanie Deutsch, WA Rental Assn.; Megan Schrader, TechNet.

OTHER: Carl Gipson, AT&T.

Persons Signed in to Testify But Not Testifying: No one.