SENATE BILL REPORT
2ESHB 1094

As of February 23, 2016

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; 2/15/16, 87-10.
Committee Activity: Law & Justice: 2/23/16.

SENATE COMMITTEE ON LAW & JUSTICE

Staff: Aldo Melchiori (786-7439)

Background: Biometric Information. The term "biometric" may refer to a measurable biological or behavioral characteristic that can be used for automated recognition, or to the process by which automated methods recognize an individual based on measurable biological and behavioral characteristics.

Establishing an Individual's Identity. Data systems may establish the unique identity of an individual through a composite of various kinds of personally identifiable information (PII), including biographical information such as name and date of birth, documents such as a birth certificate, personal life history and knowledge such as a mother's maiden name, and physiological information such as biometric characteristics.

Federal Regulation. The Federal Trade Commission Act prohibits unfair and deceptive practices in trade or commerce and authorizes the Federal Trade Commission to bring enforcement actions against violators. No federal law comprehensively regulates the collection of a person's biometric data for commercial purposes. There are a number of federal laws that establish standards for how governmental and commercial entities can collect, disclose, and use PII. Some regulate the collection of PII by specific industries (such as banking, health care, or communications) and others address specific types of PII (such as financial information, credit reports, or health care information). The federal Gramm-Leach Bliley Act of 1999 (GLBA) requires companies that offer consumers financial products or services like loans, financial or investment advice, or insurance to explain their information-sharing practices to their customers and to safeguard "nonpublic personal information."

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 the GLBA, "nonpublic personal information" is personally-identifiable financial information provided by a consumer to a financial institution resulting from any transaction with the consumer or any service performed for the consumer or otherwise obtained by the financial institution.

State Regulation. No state law comprehensively regulates the collection of a person's biometric data for commercial purposes. Under state data breach notification law, any person, business, or agency that owns or licenses computerized data that includes personal information must notify possibly affected persons when security of the system is breached and personal information may have been acquired by an unauthorized person. "Personal information" is defined as an individual's first name or first initial and last name in combination with one or more of the following data elements: Social Security number, driver's license number or Washington identification card number; or account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Covered entities such as financial institutions that comply with applicable federal laws, like the GLBA, are deemed to have complied with Washington's data breach notification law.

Enhanced Driver's Licenses. The Department of Licensing uses a one-to-many facial biometric matching system. It measures characteristics such as the distance between pupils and the size and shape of facial features that are difficult to alter, such as eye sockets, cheekbones, and the sides of the mouth. An applicant for an enhanced driver's license provides a biometric identifier that must be used solely for the purpose of verifying the identity of a cardholder or determining whether a person has been issued a license, permit, or identicard under a different name or names.

Washington Consumer Protection Act. The Consumer Protection Act (CPA) prohibits unfair methods of competition or unfair or deceptive practices in the conduct of any trade or commerce. The CPA may generally be enforced by private legal action or through a civil action by the Office of the Attorney General. Any person injured by a violation of the CPA may seek actual damages, costs, and attorneys' fees. The court may triple the amount of damages awarded up to $25,000.

Summary of Bill: "Biometric identifier" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voice print, eye retinas or irises, or other unique biological characteristic, which are used by the person or licensee to uniquely authenticate an individual's identity when the individual accesses a system or account. "Enroll" means to collect a biometric sample of an individual, convert it into a reference template, and store it in the biometric system's database for later comparison. "Person" means any individual, partnership, corporation, limited liability company, other organization, or any combination thereof.

"Commercial purpose" is a purpose in furtherance of the sale or disclosure of biometric data for the purpose of marketing goods or services when such goods or services are unrelated to the initial commercial transaction in which a person first gains possession of an individual's biometric identifier. "Commercial purpose" does not include a "security purpose," such as preventing shoplifting, fraud, or other misappropriation.

A person may not enroll a biometric identifier of an individual in a database for a commercial purpose without providing clear and conspicuous notice and obtaining the individual's affirmative consent. A person who possesses a biometric identifier that has been enrolled for a commercial purpose to take reasonable care to guard against unauthorized access. The biometric identifier may be retained no longer than reasonably necessary to effectuate the purpose for which an individual provided consent, comply with law, or protect against fraud, crime, security threats, or other liabilities. A person who has enrolled a biometric identifier may not sell, lease, or otherwise disclose the biometric identifier to another person for a commercial purpose, unless the disclosure is consistent with the original notice and consent, or an exception applies.

Disclosure to a third party is permitted when:

- necessary to provide a product or service requested by the individual;
- necessary to effect a financial transaction and the third party maintains confidentiality of the biometric data and does not further disclose it;
- required or expressly authorized by law, administrative code, or court order;
- made in good faith in response to a request from law enforcement; or
- made to a third party who contractually promises that it will not be further disclosed or enrolled for a commercial purpose inconsistent with the original notice and consent.

If the biometric identifier has been anonymized so as to prevent the possibility of ascertaining the identity of a unique individual, the limitations on disclosure and retention are inapplicable. The restrictions do not apply in any manner to a financial institution or an affiliate that is subject to Title V of the federal Gramm-Leach-Bliley Act. The act may not be construed as expanding or limiting the authority of a law enforcement officer acting within the scope of his or her authority.

The Attorney General may bring an action to enforce a material violation under the Consumer Protection Act. In such action, the Attorney General does not need to prove that the violation is unreasonable in relation to the development and preservation of business and does not need to prove that the violation is an unfair or deceptive act in trade or commerce and an unfair method of competition.

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: A lot of hard work was done during the interim to improve the bill. The premise of the bill is to require consent before biometric data collection, limit its use, and provide for deletion of that data when it is no longer needed.

CON: Different retailers and businesses commonly use different language from that used in the bill. Care should be taken to do this correctly because other states are going to use

Washington as a model. More technical input needs to be acquired from people with technical expertise. We need to acknowledge privacy concerns, but this bill has not been fully vetted. The bill has evolved too quickly and it needs more work. Biometric data is not inherently bad if it is used properly.

OTHER: The bill needs some clarifying amendments to make it work as intended.

Persons Testifying: PRO: Representative Morris, prime sponsor;

CON: Michael Schutzler, Washington Tech Industry Assn.; Joanie Deutsch, Washington Retail Association; Bob Battles, AWB; Megan Schrader, TechNet

OTHER: Mitch Barker, WASPC

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