HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: HB 1153 Biometric Information Privacy
SPONSOR(S): DuBose
TIED BILLS: **IDEN./SIM. BILLS:** SB 1270

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Business & Professions Subcommittee	11 Y, 1 N	Wright	Anstead
2) Civil Justice Subcommittee			
3) Commerce Committee			

SUMMARY ANALYSIS

"Biometric data" is a term for a measurable biological and behavioral characteristic that can be used for automatic recognition. Biometric data is used in the private sector to help verify employee information and hours worked, make advertising more effective, help social media users identify and tag other users, and enhance security by controlling access to sensitive locations. Biometric technology generally makes these tasks easier, more efficient, and more accurate.

The bill requires that a private entity:

- in possession of biometric data (defined as retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry) must have a written policy establishing a retention schedule and guidelines for permanently destroying such data.
- may not collect, capture, purchase, receive through trade, or otherwise obtain biometric data unless it informs the subject that the data is being stored and the manner of storage, and receives a written release from the subject.
- may not profit from a person's biometric data.
- may not disseminate a person's biometric data unless the subject consents, is authorized by the subject, or is required by law or a valid warrant or subpoena.
- must store, transmit, and protect biometric data with a reasonable standard of care and in a manner as or more protective as other confidential and sensitive information.

The bill provides a private cause of action, with relief including:

- liquidated damages of $1,000 or actual damages, whichever is greater, against a private entity that negligently violates the Act;
- liquidated damages of $5,000 or actual damages, whichever is greater, against a private entity that intentionally or recklessly violates the Act;
- reasonable attorneys' fees and costs; and
- other relief, including an injunction, as the court deems appropriate.

The bill does not have a fiscal impact on state or local governments.

The bill has an effective date of October 1, 2019.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Background

"Biometric data" is a term for a measurable biological and behavioral characteristic that can be used for automatic recognition. Common biometrics include fingerprint, facial recognition, iris, voice, signature, and hand geometry.[1]

Biometric data is used in the public sector to monitor border security, identify criminals, combat terrorism, and eliminate identity fraud. In the private sector, biometrics can help verify employee information and hours worked, make advertising more effective, help social media users identify and tag other users, and enhance security by controlling access to sensitive locations. Biometric technology generally makes these tasks easier and more efficient and accurate.[2]

Some specific examples of private entity use of biometric data are the Google Arts & Culture app matching a user's facial structure to one of many famous portraits,[3] and Walt Disney World employing fingerprint scanners at entry points for ticket verification.[4]

Biometric Data Legislation

Federal Laws

There is not a federal law which expressly regulates the commercial use of biometric data.[5] Certain federal laws do address the collection, use, and sale of personal information by private-sector companies and could potentially restrict, in certain circumstances, the collection of biometric data. For example, provisions in the Driver's Privacy Protection Act restrict state motor vehicle bureaus from selling drivers' license photographs and associated information to private parties. Also, the Gramm-Leach-Bliley Act and Health Insurance Portability and Accountability Act potentially could restrict the ability of banks and health care providers to share data collected with facial recognition technology if those data were to fall within the laws' definitions of protected information.[6]

Other States

Three states, Illinois, Texas, and Washington, have enacted specific privacy measures for biometric data held by a private entity.

In Illinois, under the Biometric Information Privacy Act (BIPA), a private entity:

- in possession of biometric data (defined as retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry) must have a written policy establishing a retention schedule and guidelines for permanently destroying such data.

[1] Samantha Moodie, *Facial Recognition and Biometrics*, National Conference of State Legislatures Legisbrief, Nov. 2015, http://www.ncsl.org/LinkClick.aspx?fileticket=IE4xzQZma5M%3D&tabid=29861&portalid=1 (last visited Mar. 8, 2019).
[2] *Id*.
[3] Hamza Shaban, *A Google app that matches your face to artwork is wildly popular. It's also raising privacy concerns*., Washington Post (January 17, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/01/16/google-app-that-matches-your-face-to-artwork-is-wildly-popular-its-also-raising-privacy-concerns/?utm_term=.ad4e7640114b (last visited Mar. 8, 2019).
[4] Jill Disis, *Disney World scanning toddlers' fingers to stop ticket fraud*, CNN Business (Sept. 7, 2016), https://money.cnn.com/2016/09/07/news/companies/disney-world-finger-scan/index.html (last visited Mar. 8, 2019).
[5] Carissa Ratanaphanyarat, *Biometric Privacy Laws: Do They Exist and Why Should You Care?*, NextAdvisor Blog, Sept. 6 , 2018, https://www.nextadvisor.com/blog/biometric-privacy-laws/ (last visited Mar. 8, 2019).
[6] U.S. Gov't Accountability Office, GAO-15-621, Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law 33 (July 2015), https://www.gao.gov/assets/680/671764.pdf (last visited Mar. 8, 2019).

- may not collect, capture, purchase, receive through trade, or otherwise obtain biometric data unless it informs the subject that the data is being stored and the manner of storage, and receives a written release from the subject.
- may not profit from a person's biometric data.
- may not disseminate a person's biometric data unless the subject consents, is authorized by the subject, or is required by law or a valid warrant or subpoena.
- must store, transmit, and protect biometric data with a reasonable standard of care and in a manner as or more protective as other confidential and sensitive information.[7]

Illinois provides a private cause of action for violations of BIPA, with relief including:
- liquidated damages of $1,000 or actual damages, whichever is greater, against a private entity that negligently violates BIPA;
- liquidated damages of $5,000 or actual damages, whichever is greater, against a private entity that intentionally or recklessly violates BIPA;
- reasonable attorneys' fees and costs; and
- other relief, including an injunction, as the court deems appropriate.[8]

Texas and Washington both have a similar law to Illinois in its function by requiring consent for private entity use of biometric data, and mandating standards for retention, destruction, use, and care of such data. However, Texas and Washington do not provide a private cause of action.[9]

Washington defines biometric data differently than Illinois and Texas:

> "data generated by automatic measurements of an individual's biological characteristics, such as fingerprints, voiceprints, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual," and does not specifically provide for a "scan of hand or face geometry."[10]

All three states have cited privacy concerns as a main reason for regulating how private entities use biometric data. Illinois found that biometrics are unlike other unique identifiers that are used to access sensitive information. Biometrics are biologically unique to the individual, and when such data is compromised, the individual has no recourse and is at heightened risk for identity theft.[11] Texas noted that a record of a biometric identifier can be used by identity thieves to impersonate the owner in business transactions or other contexts.[12] Washington highlighted the need for consent and notice when private entities collect data from an individual.[13]

Litigation of the Illinois BIPA Law

Because Illinois has granted a private cause of action for violations of BIPA, there have been several lawsuits claiming damages for privacy and use violations.

On January 25, 2019, the Illinois Supreme Court found that an individual does not need to allege an actual injury or adverse effect, beyond violation of their rights under BIPA, to qualify as an aggrieved party. Therefore, they are able to seek liquidated damages or injunctive relief under the Act.[14]

---

[7] 740 Ill. Comp. Stat. 14/10, 14/15 (2008).
[8] 740 Ill. Comp. Stat. 14/20 (2008).
[9] Tex. Bus. & Com. Code Ann. § 503.001 (2017).
[10] Wash. Rev. Code § 19.375.010-040 (2018).
[11] 740 Ill. Comp. Stat. 14/5 (2008).
[12] Texas Legislature, Bill Analysis of C.S.H.B. 3186, 2009, https://capitol.texas.gov/tlodocs/81R/analysis/pdf/HB03186H.pdf#navpanes=0 (last visited Mar. 8, 2019).
[13] Wash. Rev. Code § 19.375.900 (2018).
[14] *Rosenbach v. Six Flags Entertainment Corporation*, 2019 IL 123186.

Other cases are still ongoing, but court documents tend to support the notion that an individual in Illinois has a valid cause of action if their biometric data is taken without consent by a private entity, including out-of-state entities.[15] Courts have yet to render a definitive opinion on the applicability of the Dormant Commerce Clause.[16]

Florida Personal Information Privacy Laws

Florida Laws Concerning Biometric Data

Florida does not have a broad law specific to regulating biometric data privacy held by private entities, but there are laws related to biometric information use and privacy in the following areas:

- There is a public records exemption for biometric identification information held by an agency, defined in the law as "any record of friction ridge detail, fingerprints, palm prints, and footprints."[17]
- It is a crime to willfully and without authorization fraudulently use or possesses with intent to use; without consent; personal identification information, which includes biometric data defined as fingerprint, voice print, retina or iris image, or other unique physical representation; for pecuniary benefit or the purpose of harassment.[18]
- An education agency or institution may not collect, obtain or retain biometric information of a student or a student's parent or sibling. Biometric information in this instance includes fingerprint or hand scan, retina or iris scan, voice print, or facial geometry scan.[19]
- The Criminal Justice Information Program within the Department of Law Enforcement is tasked with creating a program to, among other responsibilities, maintain a statewide automated biometric identification system to read, classify, match and store fingerprints, palm prints, and facial images for the administration of criminal justice. This system is also used for criminal background screenings.[20]

Florida Information Protection Act

In 2014, Florida passed the Florida Information Protection Act (FIPA).[21] FIPA requires businesses and government entities which hold personal information to take reasonable measures to protect such information and report data breaches to affected consumers.[22]

FIPA defines "personal information" as:

- online account information, such as security questions and answers, email addresses and passwords;
- an individual's first name or first initial and last name in combination with any one or more of the following:
    - A social security number;
    - A driver license or similar identity verification number issued on a government document;
    - A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;

[15] *Rivera v. Google, Inc.*, 238 F.Supp.3d 1088 (N.D. Ill. 2017).; *In re Facebook Biometric Information Privacy Litigation*, 185 F.Supp.3d 1155 (N.D. Cal. (2016).; *Norberg v. Shutterfly, Inc.*, 152 F.Supp.3d 1103 (N.D. Ill. 2015).
[16] *Id*.
[17] S. 119.071(5)(g), F.S.
[18] S. 817.568, F.S.
[19] S. 1002.222, F.S.
[20] S. 943.05, F.S.
[21] S. 501.171, F.S.; Fla. SB 1524 (2014).
[22] Florida Office of the Attorney General, *How to Protect Yourself: Data Security*, http://myfloridalegal.com/pages.nsf/Main/53D4216591361BCD85257F77004BE16C (last visited Mar. 8, 2019).

- Any medical history information; or
- An individual's health insurance identification numbers.[23]

Personal information does not include information:
- about an individual that has been made publicly available by a federal, state, or local governmental entity; or
- that is encrypted, secured, or modified to remove elements that personally identify an individual or that otherwise renders the information unusable.[24]

If a breach of personal information occurs, the business or government entity or a third party of such entity in possession of the information must provide notice to the affected individual, the Department of Legal Affairs, and credit reporting agencies of such breach, under certain circumstances.[25]

FIPA does not give a private cause of action, but does authorize enforcement actions under Florida's Unfair and Deceptive Trade Practices Act for any statutory violations.[26]

Effect of the Bill

The bill designates "Florida Biometric Information Privacy Act" as the short title.

The bill provides the following definitions:
- "Biometric identifier" means a retina or iris scan, fingerprint, voice print, or scan of hand or face geometry. The term does not include any of the following:
  - Writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color;
  - Donated organs, tissues, parts, or blood or serum that is stored on behalf of recipients, or potential recipients, of living or cadaveric transplants and that are obtained by or stored by a federally designated organ procurement organization;
  - Information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996; or
  - An X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.
- "Biometric information" means any information, regardless of the manner in which it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. The term does not include information derived from items or procedures excluded from the definition of biometric identifiers as specified in paragraph (a).
- "Confidential and sensitive information" means personal information that can be used to uniquely identify an individual or an individual's account or property which includes, but is not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver license number, a Florida identification card number, or a social security number.
- "Private entity" means any individual, partnership, corporation, limited liability company, association, or other group. The term does not include a state or local governmental agency or any state court, a clerk of the court, or a judge or justice thereof.
- "Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.

[23] S. 501.171(1)(g)1., F.S.; OAG *supra* note 22.
[24] S. 501.171(1)(g)2., F.S.
[25] S. 501.171(3)-(6), F.S.
[26] S. 501.171(9), (10), F.S.; OAG *supra* note 22.

The bill requires private entities in possession of biometric identifiers or information to develop a publicly available written policy which establishes a retention schedule and guidelines for permanently destroying such identifiers or information within 3 years of the last time the individual had interaction with the private entity. Private entities may not deviate from its established retention schedule and destruction guidelines unless directed to do so by a valid warrant or subpoena issued by a court of competent jurisdiction.

The bill provides that private entities may not collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or information unless the private entity:

- Informs the subject or the subject's legally authorized representative in writing that such identifier or information is being collected or stored;
- Informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of time such identifier or information is being collected, stored, and used; and
- Receives a written release executed by the subject or the subject's legally authorized representative.

A private entity in possession of a biometric identifier or information may not sell, lease, trade or otherwise profit from a person's or a customer's biometric identifier or information.

A private entity in possession of a biometric identifier or information may not disclose or otherwise disseminate a person's or a customer's biometric identifier or information unless:

- the subject of such information or such subject's legally authorized representative consents to the disclosure;
- the disclosure completes a financial transaction requested or authorized by the subject of such information or such subject's legally authorized representative;
- the disclosure is required by federal or state law, or local ordinance; or
- the disclosure is required pursuant to a valid warrant or subpoena issued by a court of valid jurisdiction.

A private entity in possession of a biometric identifier or information must store, transmit, and protect from disclosure all such identifiers and information:

- using the reasonable standard of care within the private entity's industry; and
- in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

The bill creates a cause of action against private entities who violate the act. A prevailing party may recover for each violation:

- liquidated damages of $1,000 or actual damages, whichever is greater, against a private entity that negligently violates the act;
- liquidated damages of $5,000 or actual damages, whichever is greater, against a private entity that intentionally or recklessly violates the act;
- reasonable attorney fees; and
- other relief, including an injunction, as the court deems appropriate.

The bill states that the act may not be construed to:

- impact the admission or discovery of biometric identifiers and information in any action of any kind in any court, or before any tribunal, board, agency, or person;
- conflict with the federal Health Insurance Portability and Accountability Act of 1996 and any regulations promulgated pursuant to that act;
- apply to a contractor, subcontractor, or agent of a state agency or local unit of government when working for that state agency or local unit of government; or

- apply to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and any regulations promulgated pursuant to that act.

The bill is very similar to the Illinois BIPA law.

The effective date of the bill Is October 1, 2019.

B. SECTION DIRECTORY:

Section 1 Provides definitions, requirements for private entities related to biometric data, and a cause of action for an injured party.

Section 2 Provides an effective date.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   None.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

   None.

2. Expenditures:

   None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

Private entities will not be allowed to profit off of consumer's biometric data and must create standards for retention, destruction, use, and care of such data, which may require an increase in private resources. However, consumers may see a decrease in identity theft situations, which may benefit consumers and others by limiting fraudulent activities.

D. FISCAL COMMENTS:

None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

   Not applicable. This bill does not appear to affect county or municipal governments.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

Not applicable.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES