

By Senator Farmer

34-01069-19

20191270__

1 A bill to be entitled
2 An act relating to biometric information privacy;
3 creating s. 501.172, F.S.; providing a short title;
4 providing definitions; establishing requirements and
5 restrictions on private entities as to the use,
6 collection, and maintenance of biometric identifiers
7 and biometric information; creating a private cause of
8 action for relief for violations of the act; providing
9 for construction; providing an effective date.

10
11 Be It Enacted by the Legislature of the State of Florida:

12
13 Section 1. Section 501.172, Florida Statutes, is created to
14 read:

15 501.172 Biometric information privacy.-

16 (1) SHORT TITLE.-This section may be cited as the "Florida
17 Biometric Information Privacy Act."

18 (2) DEFINITIONS.-As used in this section, the term:

19 (a) "Biometric identifier" means a retina or iris scan,
20 fingerprint, voice print, or scan of hand or face geometry. The
21 term does not include any of the following:

22 1. Writing samples, written signatures, photographs, human
23 biological samples used for valid scientific testing or
24 screening, demographic data, tattoo descriptions, or physical
25 descriptions such as height, weight, hair color, or eye color.

26 2. Donated organs, tissues, parts, or blood or serum that
27 is stored on behalf of recipients, or potential recipients, of
28 living or cadaveric transplants and that are obtained by or
29 stored by a federally designated organ procurement organization.

34-01069-19

20191270__

30 3. Information captured from a patient in a health care
31 setting or information collected, used, or stored for health
32 care treatment, payment, or operations under the federal Health
33 Insurance Portability and Accountability Act of 1996.

34 4. An X-ray, roentgen process, computed tomography, MRI,
35 PET scan, mammography, or other image or film of the human
36 anatomy used to diagnose, prognose, or treat an illness or other
37 medical condition or to further validate scientific testing or
38 screening.

39 (b) "Biometric information" means any information,
40 regardless of the manner in which it is captured, converted,
41 stored, or shared, based on an individual's biometric identifier
42 used to identify an individual. The term does not include
43 information derived from items or procedures excluded from the
44 definition of biometric identifiers as specified in paragraph
45 (a).

46 (c) "Confidential and sensitive information" means personal
47 information that can be used to uniquely identify an individual
48 or an individual's account or property which includes, but is
49 not limited to, a genetic marker, genetic testing information, a
50 unique identifier number to locate an account or property, an
51 account number, a PIN number, a pass code, a driver license
52 number, a Florida identification card number, or a social
53 security number.

54 (d) "Private entity" means any individual, partnership,
55 corporation, limited liability company, association, or other
56 group. The term does not include a state or local governmental
57 agency or any state court, a clerk of the court, or a judge or
58 justice thereof.

34-01069-19

20191270__

59 (e) "Written release" means informed written consent or, in
60 the context of employment, a release executed by an employee as
61 a condition of employment.

62 (3) REQUIREMENTS OF PRIVATE ENTITIES.-

63 (a) A private entity that is in possession of biometric
64 identifiers or biometric information shall develop a publicly
65 available written policy establishing a retention schedule and
66 guidelines for permanently destroying biometric identifiers and
67 biometric information upon satisfaction of the initial purpose
68 for collecting or obtaining such identifiers or information or
69 within 3 years after the individual's last interaction with the
70 private entity, whichever occurs first. Absent a valid warrant
71 or subpoena issued by a court of competent jurisdiction, a
72 private entity in possession of biometric identifiers or
73 biometric information must comply with its established retention
74 schedule and destruction guidelines.

75 (b) A private entity may not collect, capture, purchase,
76 receive through trade, or otherwise obtain a person's or a
77 customer's biometric identifier or biometric information unless
78 the private entity:

79 1. Informs the subject or the subject's legally authorized
80 representative in writing that a biometric identifier or
81 biometric information is being collected or stored;

82 2. Informs the subject or the subject's legally authorized
83 representative in writing of the specific purpose and length of
84 term for which a biometric identifier or biometric information
85 is being collected, stored, and used; and

86 3. Receives a written release executed by the subject of
87 the biometric identifier or biometric information or the

34-01069-19

20191270__

88 subject's legally authorized representative.

89 (c) A private entity in possession of a biometric
90 identifier or biometric information may not sell, lease, trade,
91 or otherwise profit from a person's or a customer's biometric
92 identifier or biometric information.

93 (d) A private entity in possession of a biometric
94 identifier or biometric information may not disclose or
95 otherwise disseminate a person's or a customer's biometric
96 identifier or biometric information unless:

97 1. The subject of the biometric identifier or biometric
98 information or the subject's legally authorized representative
99 consents to the disclosure;

100 2. The disclosure completes a financial transaction
101 requested or authorized by the subject of the biometric
102 identifier or the biometric information or the subject's legally
103 authorized representative;

104 3. The disclosure is required by state or federal law or
105 local ordinance; or

106 4. The disclosure is required pursuant to a valid warrant
107 or subpoena issued by a court of competent jurisdiction.

108 (e) A private entity in possession of a biometric
109 identifier or biometric information shall store, transmit, and
110 protect from disclosure all biometric identifiers and biometric
111 information:

112 1. Using the reasonable standard of care within the private
113 entity's industry; and

114 2. In a manner that is the same as or more protective than
115 the manner in which the private entity stores, transmits, and
116 protects other confidential and sensitive information.

34-01069-19

20191270__

117 (4) CAUSE OF ACTION.—Any person aggrieved by a violation of
118 this section has a cause of action in circuit court against an
119 offending party. A prevailing party may recover for each
120 violation:

121 (a) Liquidated damages of \$1,000 or actual damages,
122 whichever amount is greater, against a private entity that
123 negligently violates any provision in subsection (3).

124 (b) Liquidated damages of \$5,000 or actual damages,
125 whichever amount is greater, against a private entity that
126 intentionally or recklessly violates any provision in subsection
127 (3).

128 (c) Reasonable attorney fees.

129 (d) Other relief, including an injunction, as the court
130 deems appropriate.

131 (5) CONSTRUCTION.—This section may not be construed to:

132 (a) Impact the admission or discovery of biometric
133 identifiers and biometric information in any action of any kind
134 in any court, or before any tribunal, board, agency, or person;

135 (b) Conflict with the federal Health Insurance Portability
136 and Accountability Act of 1996 and any regulations promulgated
137 pursuant to that act;

138 (c) Apply to a contractor, subcontractor, or agent of a
139 state agency or local unit of government when working for that
140 state agency or local unit of government; or

141 (d) Apply to a financial institution or an affiliate of a
142 financial institution that is subject to Title V of the federal
143 Gramm-Leach-Bliley Act of 1999 and any regulations promulgated
144 pursuant to that act.

145 Section 2. This act shall take effect October 1, 2019.