To regulate the collection, retention, disclosure, and destruction of biometric information, and for other purposes.

---

IN THE SENATE OF THE UNITED STATES

Mr. MERKLEY (for himself and Mr. SANDERS) introduced the following bill; which was read twice and referred to the Committee on

---

A BILL

To regulate the collection, retention, disclosure, and destruction of biometric information, and for other purposes.

1 Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

2 SECTION 1. SHORT TITLE.

3 This Act may be cited as the "National Biometric Information Privacy Act of 2020".

4 SEC. 2. DEFINITIONS.

5 In this Act:

6 (1) BIOMETRIC IDENTIFIER.—The term "biometric identifier"—

7 (A) includes—
(i) a retina or iris scan;
(ii) a voiceprint;
(iii) a faceprint (including any faceprint derived from a photograph);
(iv) fingerprints or palm prints; and
(v) any other uniquely identifying information based on the characteristics of an individual’s gait or other immutable characteristic of an individual;

(B) does not include 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;

(C) does not include donated organs, tissues, or parts or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a Federally designated organ procurement agency;

(D) does not include information captured from a patient in a health care setting for a medical purpose or information collected, used, or stored for health care treatment, payment, or
operations under the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191); and

(E) does not include 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.

(2) CONFIDENTIAL AND SENSITIVE INFORMATION.—The term “confidential and sensitive information”—

(A) means personal information that can be used to uniquely identify an individual or an individual’s account or property; and

(B) includes genetic markers, genetic testing information, unique identifier numbers to locate accounts or property, account numbers, personal identification numbers, pass codes, driver’s license numbers, or Social Security numbers.

(3) PRIVATE ENTITY.—The term “private entity”—
(A) means any individual, partnership, corporation, limited liability company, association, or other group, however organized; and

(B) does not include any Federal, State, or local government agency or academic institution.

(4) WRITTEN RELEASE.—The term “written release” means—

(A) specific, discrete, freely given, unambiguous, and informed written consent given by an individual who is not under any duress or undue influence of an entity or third party at the time such consent is given; or

(B) in the context of employment, a release executed by an employee as a condition of employment.

SEC. 3. COLLECTION, RETENTION, DISCLOSURE, AND DESTRUCTION OF BIOMETRIC INFORMATION.

(a) WRITTEN POLICY.—

(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, any private entity in possession of biometric identifiers or biometric information concerning an individual shall develop and make available to the public a written policy establishing a retention schedule and guidelines
for permanently destroying such biometric identifiers and biometric information not later than the earlier of—

(A) the date on which the initial purpose for collecting or obtaining such identifiers or information has been satisfied, if the individual from whom the biometric information was collected—

(i) freely consented to the original purpose for such collection; and

(ii) could have declined such collection without consequence; or

(B) 1 year after the individual’s last intentional interaction with the private entity.

(2) COMPLIANCE.—Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information shall comply with the retention schedule and destruction guidelines established pursuant to paragraph (1).

(b) LIMITATIONS.—

(1) IN GENERAL.—A private entity may not collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifier or biometric information unless—
(A) the entity requires the identifier or information—

(i) to provide a service for the person or customer; or

(ii) for another valid business purpose specified in the written policy published pursuant to section 3; and

(B) the entity first—

(i) informs the person or customer, or his or her legally authorized representative, in writing—

(I) that such biometric identifier or biometric information is being collected or stored; and

(II) of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(ii) receives a written release executed by the subject of the biometric identifier or biometric information or by the subject’s legally authorized representative.

(2) WRITTEN RELEASE.—A written release under paragraph (1)(B)—
(A) may not be sought through, as a part of, or otherwise combined with any other consent or permission seeking instrument or function;

(B) may not be combined with an employment contract; and

(C) if it involves a minor, may only be obtained through the minor’s parent or guardian.

(e) **PROHIBITED ACTS.**—A private entity in possession of a biometric identifier or biometric information may not sell, lease, trade, use for advertising purposes, or otherwise profit from a person’s or a customer’s biometric identifier or biometric information.

(d) **DISCLOSURE.**—A private entity in possession of a biometric identifier or the biometric information of a person, including a consumer, job applicant, employee, former employee, or contractor, may not disclose, redisclose, sell, lease, trade, use for advertising purposes, otherwise disseminate, or profit from such biometric identifier or biometric information unless—

(1) the subject of the biometric identifier or biometric information, or the subject’s legally authorized representative, provides a written release to such specified action immediately prior to such disclosure or redisclosure, including a description of—
(A) the data that will be disclosed;

(B) the reason for such disclosure; and

(C) the recipients of such data

(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject’s legally authorized representative; or

(3) the disclosure or redisclosure—

(A) is required by Federal, State, or municipal law; or

(B) is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(e) CONDITIONS.—A private entity in possession of a biometric identifier or biometric information shall store, transmit, and protect from disclosure all biometric identifiers and biometric information—

(1) using the reasonable standard of care within the private entity’s industry; and

(2) 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.
(f) **Right to Know.**—Any business that collects, uses, shares, or sells biometric identifiers or biometric information, upon the request of an individual, shall disclose, free of charge, any such information relating to such individual collected during the preceding 12-month period, including—

1. the categories of personal information;
2. specific pieces of personal information;
3. the categories of sources from which the business collected personal information;
4. the purposes for which the business uses the personal information;
5. the categories of third parties with whom the business shares the personal information; and
6. the categories of information that the business sells or discloses to third parties.

**SEC. 4. CAUSE OF ACTION.**

(a) **In General.**—Any individual aggrieved by a violation of section 3 may bring a civil action in a court of competent jurisdiction against a private entity that allegedly committed such violation. Any such violation constitutes an injury-in-fact and a harm to any affected individual.

(b) **Admissibility.**—Except in a judicial investigation or proceeding alleging a violation of section 3, infor-
1 mation obtained in violation of section 3 is not admissible
2 by the Federal Government in any criminal, civil, adminis-
3 trative, or other investigation or proceeding.
4 (c) RIGHT TO SUE.—An individual described in sub-
5 section (a) may institute legal proceedings against a pri-
6 vate entity alleged to have violated section 3 for the relief
7 described in subsection (e) in any court of competent juris-
8 diction.
9 (d) ENFORCEMENT BY STATE ATTORNEYS GEN-
10 ERAL.—The chief law enforcement officer of a State, or
11 any other State officer authorized by law to bring actions
12 on behalf of the residents of a State, may bring a civil
13 action, as parens patriae, on behalf of the residents of
14 such State in an appropriate district court of the United
15 States to enforce this Act if the chief law enforcement offi-
16 cer or other State officer has reason to believe that the
17 interests of the residents of the State have been or are
18 being threatened or adversely affected by a violation of
19 section 3.
20 (e) FORMS OF RELIEF.—
21 (1) IN GENERAL.—A plaintiff bringing a civil
22 action under this section may recover—
23 (A)(i) for the negligent violations of any
24 provision of section 3, the greater of—
(I) $1,000 in liquidated damages per violation; or

(II) the actual damages suffered by the plaintiff; or

(ii) for the intentional or reckless violation of any provision of section 3, the sum of—

(I) the actual damages suffered by the plaintiff; and

(II) any punitive damages awarded by the court, which shall be limited to $5,000 per violation;

(B) reasonable attorneys’ fees and costs, including expert witness fees and other litigation expenses; and

(C) other relief, including an injunction, as the court may deem appropriate.

(2) Specific performance.—A court may require a private entity to permanently destroy the biometric identifiers, biometric information, or confidential and sensitive information of a plaintiff under this section.

SEC. 5. RULES OF CONSTRUCTION.

Nothing in this Act may be construed—

(1) to impact the admission or discovery of biometric identifiers and biometric information in any
action of any kind in any court, or before any tribunal, board, agency, or person;

(2) to conflict with the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191);

(3) to conflict with title V of the Federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.);

(4) to apply to a contractor, subcontractor, or agent of a Federal, State, or local government agency in the course of employment with such agency; or

(5) to preempt or supersede any Federal, State, or local law that imposes a more stringent limitation than the limitations described in section 3.