116TH CONGRESS
1ST SESSION

S. 847

To prohibit certain entities from using facial recognition technology to identify or track an end user without obtaining the affirmative consent of the end user, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MARCH 14, 2019

Mr. BLUNT (for himself and Mr. SCHATZ) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

A BILL

To prohibit certain entities from using facial recognition technology to identify or track an end user without obtaining the affirmative consent of the end user, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Commercial Facial Recognition Privacy Act of 2019''.

SEC. 2. DEFINITIONS.

In this Act:

(1) AFFIRMATIVE CONSENT.—The term ''affirmative consent'' means the consent of an end user that involves an individual, voluntary, and explicit agreement to the collection and data use policies of a controller.

(2) CONTROLLER.—The term ''controller'' means a covered entity that, alone or jointly with others, determines the purposes and means of the processing of facial recognition data.

(3) COVERED ENTITY.—The term ''covered entity''—

(A) means any person, including corporate affiliates, that collects, stores, or processes facial recognition data; and

(B) does not include—

(i) the Federal Government or any State or local government;

(ii) a law enforcement agency;

(iii) a national security agency; or

(iv) an intelligence agency.

(4) END USER.—The term ''end user'' means an individual.

(5) FACIAL RECOGNITION TECHNOLOGY.—The term ''facial recognition technology'' means technology that—

(A) analyzes facial features in still or video images; and

(B)(i) is used to assign a unique, persistent identifier; or

(ii) is used for the unique personal identification of a specific individual.

(6) FACIAL RECOGNITION DATA.—The term ''facial recognition data'' means any unique attribute or feature of the face of an end user that is used by facial recognition technology to assign a unique, persistent identifier or for the unique personal identification of a specific individual.

(7) PROCESS.—The term ''process'' means any operation that is performed on facial recognition data, including collection, creation, generation, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, transfer, dissemination or otherwise making available, combination, erasure, or destruction.

(8) PROCESSOR.—The term ''processor'' means a covered entity that processes facial recognition data on behalf of a controller.

(9) SECURITY APPLICATION.—The term ''security application'' means loss prevention and any

other application intended to detect or prevent criminal activity, including shoplifting and fraud.

(10) UNAFFILIATED THIRD PARTY.—The term ''unaffiliated third party'' means any person other than—

(A) a user of a product or service of a covered entity;

(B) an employee of a covered entity;

(C) a person under common control or ownership with a covered entity; or

(D) a person to whom—

(i) an end user directed a covered entity to disclose information derived from facial recognition technology; or

(ii) information derived from facial recognition technology was disclosed with the affirmative consent of an end user.

SEC. 3. PROHIBITED CONDUCT.

(a) IN GENERAL.—Except as provided in subsection (e), it shall be unlawful for a controller to knowingly—

(1) use facial recognition technology to collect facial recognition data, unless the controller—

(A) obtains from an end user affirmative consent in accordance with subsection (b); and

(B) to the extent possible, if facial recognition technology is present, provides to the end user—

(i) a concise notice that facial recognition technology is present, and, if contextually appropriate, where the end user can find more information about the use of facial recognition technology by the controller; and

(ii) documentation that includes general information that explains the capabilities and limitations of the facial recognition technology in terms that end users are able to understand;

(2) use the facial recognition technology to discriminate against an end user in violation of applicable Federal or State law;

(3) repurpose facial recognition data for a purpose that is different from those presented to the end user under paragraph (1)(A); or

(4) share the facial recognition data with an unaffiliated third party without affirmative consent that is separate from the affirmative consent required under paragraph (1)(A).

(b) CONSENT.—

(1) IN GENERAL.—When obtaining affirmative consent, a controller shall make available to an end user a notice that describes the specific practices of the processor in terms that end users are able to understand regarding the collection, storage, and use of facial recognition data, including—

(A) the reasonably foreseeable purposes, or examples, for which the processor collects and shares information derived from facial recognition technology or uses facial recognition technology;

(B) the data retention and deidentification practices of the processor; and

(C) if the controller offers the ability to review, correct, or delete information derived from facial recognition technology, the process to accomplish such actions.

(2) PROCESSOR REQUIREMENT.—If the processor and controller are not the same entity, the processor shall make easily accessible to controllers the information required under paragraph (1).

(3) CONDITIONING SERVICE ON CONSENT PROHIBITED.—If the use of facial recognition technology is not necessary for a service, no controller may—

(A) condition the service on consent by an end user to waive privacy rights; or

(B) terminate or refuse the service as a direct consequence of refusal by the end user to provide affirmative consent to the covered entity.

(c) REVIEW.—A controller, and the processor if applicable, shall employ meaningful human review prior to making any final decision based on the output of facial recognition technology if the final decision—

(1) may result in a reasonably foreseeable and material physical or financial harm to an end user; or

(2) may be unexpected or highly offensive to a reasonable end user.

(d) APPLICATION PROGRAMMING INTERFACE.—A covered entity that makes a facial recognition technology available as an online service shall make available an application programming interface to enable at least 1 third party that is legitimately engaged in independent testing to conduct reasonable tests of the facial recognition technology for accuracy and bias.

(e) EXCEPTIONS.—

(1) IN GENERAL.—Except as provided in paragraph (2), subsections (a)(1) and (b) shall not apply to controllers that use—

(A) an application that—

(i) is a product or service designed for personal file management or photo or video sorting or storage if the facial recognition technology is not used for unique personal identification of a specific individual;

(ii) involves identification of public figures for journalistic media created for public interest;

(iii) involves identification of public figures in copyrighted material for theatrical release; or

(iv) is used if there is an emergency involving imminent danger or risk of death or serious physical injury to an individual; or

(B) facial recognition data to determine whether an end user has given affirmative consent if the controller immediately and permanently destroys the facial recognition data after determining that the end user has not given affirmative consent.

(2) SECURITY APPLICATIONS.—Subsections (a)(1)(A) and (b) shall not apply to controllers that use an application that is a security application.

(3) RULE OF CONSTRUCTION.—Nothing in paragraph (1)(B) may be construed to authorize the mass scanning of faces in spaces where end users do not have a reasonable expectation that facial recognition technology is being used on them.

SEC. 4. ENFORCEMENT.

(a) UNFAIR OR DECEPTIVE ACT OR PRACTICE.—A violation of section 3 shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(b) POWERS OF COMMISSION.—

(1) IN GENERAL.—The Federal Trade Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act.

(2) PRIVILEGES AND IMMUNITIES.—Any person who violates section 3 shall be subject to the penalties and entitled to the privileges and immunities

provided in the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(c) ENFORCEMENT BY STATES.—

(1) IN GENERAL.—If the attorney general of a State has reason to believe that an interest of the residents of the State has been or is being threatened or adversely affected by a practice that violates section 3, the attorney general of the State may, as parens patriae, bring a civil action on behalf of the residents of the State in an appropriate district court of the United States to obtain appropriate relief.

(2) RIGHTS OF COMMISSION.—

(A) NOTICE TO COMMISSION.—

(i) IN GENERAL.—Except as provided in clause (iii), the attorney general of a State, before initiating a civil action under paragraph (1), shall provide written notification to the Commission that the attorney general intends to bring such civil action.

(ii) CONTENTS.—The notification required under clause (i) shall include a copy of the complaint to be filed to initiate the civil action.

(iii) EXCEPTION.—If it is not feasible for the attorney general of a State to provide the notification required under clause (i) before initiating a civil action under paragraph (1), the attorney general shall notify the Commission immediately upon instituting the civil action.

(B) INTERVENTION BY COMMISSION.—The Commission may—

(i) intervene in any civil action brought by the attorney general of a State under paragraph (1); and

(ii) upon intervening—

(I) be heard on all matters arising in the civil action; and

(II) file petitions for appeal of a decision in the civil action.

(3) INVESTIGATORY POWERS.—Nothing in this subsection may be construed to prevent the attorney general of a State from exercising the powers conferred on the attorney general by the laws of the State to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.

(4) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under paragraph (1) may be brought in—

(i) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(ii) another court of competent jurisdiction.

(B) SERVICE OF PROCESS.—In an action brought under paragraph (1), process may be served in any district in which—

(i) the defendant is an inhabitant, may be found, or transacts business; or

(ii) venue is proper under section 1391 of title 28, United States Code.

(5) ACTIONS BY OTHER STATE OFFICIALS.—

(A) IN GENERAL.—In addition to a civil action brought by an attorney general under paragraph (1), any other officer of a State who is authorized by the State to do so may bring a civil action under paragraph (1), subject to the same requirements and limitations that apply under this subsection to civil actions brought by attorneys general.

(B) SAVINGS PROVISION.—Nothing in this subsection may be construed to prohibit an authorized official of a State from initiating or continuing any proceeding in a court of the State for a violation of any civil or criminal law of the State.

SEC. 5. REGULATIONS.

(a) REGULATIONS.—Not later than 180 days after the date of enactment of this Act, the Federal Trade Commission, in consultation with the National Institute of Standards and Technology, shall promulgate regulations, in accordance with section 553 of title 5, United States Code—

(1) describing data security, minimization, and retention standards to be met at a minimum by processors;

(2) defining what is harmful and highly offensive under paragraphs (1) and (2) of section 3(c); and

(3) expanding the list of exceptions described in section 3(e) in cases where it is impossible for a controller to obtain affirmative consent from, or provide notice to, end users.

(b) CONSIDERATIONS.—In promulgating regulations under subsection (a), the Commission shall consider, among other factors—

(1) the size of the processor;

(2) the complexity of the offerings of the processor; and

(3) the nature and scope of the activities of the processor.

SEC. 6. RELATION TO STATE LAWS.

(a) IN GENERAL.—This Act shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this Act, and then only to the extent of the inconsistency.

(b) GREATER PROTECTION UNDER STATE LAW.—For purposes of this Act, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subtitle if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this Act, as determined by the Federal Trade Commission.

SEC. 7. RELATION TO OTHER PRIVACY AND SECURITY LAWS.

Nothing in this Act may be construed to—

(1) modify, limit, or supersede the operation of any privacy or security provision in any other Federal or State law (including regulations); or

(2) limit the authority of the Commission under any other provision of law.

SEC. 8. EFFECTIVE DATE.

This Act shall take effect on the date that is 180 days after the date of enactment of this Act.

○