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:

(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

(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.—

(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.—

(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

(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.

(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.

(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.

○