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.

1 *Be it enacted by the Senate and House of Representa-*

2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the "Commercial Facial

5 Recognition Privacy Act of 2019".

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1     (1) AFFIRMATIVE CONSENT.—The term "af-

2 firmative consent" means the consent of an end user

3 that involves an individual, voluntary, and explicit

4 agreement to the collection and data use policies of

5 a controller.

6     (2) CONTROLLER.—The term "controller"

7 means a covered entity that, alone or jointly with

8 others, determines the purposes and means of the

9 processing of facial recognition data.

10     (3) COVERED ENTITY.—The term "covered en-

11 tity"—

12     (A) means any person, including corporate

13 affiliates, that collects, stores, or processes fa-

14 cial recognition data; and

15     (B) does not include—

16     (i) the Federal Government or any

17 State or local government;

18     (ii) a law enforcement agency;

19     (iii) a national security agency; or

20     (iv) an intelligence agency.

21     (4) END USER.—The term "end user" means

22 an individual.

23     (5) FACIAL RECOGNITION TECHNOLOGY.—The

24 term "facial recognition technology" means tech-

25 nology that—

1    (A) analyzes facial features in still or video

2   images; and

3    (B)(i) is used to assign a unique, per-

4   sistent identifier; or

5    (ii) is used for the unique personal identi-

6   fication of a specific individual.

7   (6) FACIAL RECOGNITION DATA.—The term

8 "facial recognition data" means any unique attribute

9 or feature of the face of an end user that is used

10 by facial recognition technology to assign a unique,

11 persistent identifier or for the unique personal iden-

12 tification of a specific individual.

13   (7) PROCESS.—The term "process" means any

14 operation that is performed on facial recognition

15 data, including collection, creation, generation, re-

16 cording, organization, structuring, storage, adapta-

17 tion, alteration, retrieval, consultation, use, disclo-

18 sure, transfer, dissemination or otherwise making

19 available, combination, erasure, or destruction.

20   (8) PROCESSOR.—The term "processor" means

21 a covered entity that processes facial recognition

22 data on behalf of a controller.

23   (9) SECURITY APPLICATION.—The term "secu-

24 rity application" means loss prevention and any

1   other application intended to detect or prevent crimi-

2   nal activity, including shoplifting and fraud.

3        (10) UNAFFILIATED THIRD PARTY.—The term

4   "unaffiliated third party" means any person other

5   than—

6             (A) a user of a product or service of a cov-

7   ered entity;

8             (B) an employee of a covered entity;

9             (C) a person under common control or

10  ownership with a covered entity; or

11            (D) a person to whom—

12            (i) an end user directed a covered en-

13  tity to disclose information derived from

14  facial recognition technology; or

15            (ii) information derived from facial

16  recognition technology was disclosed with

17  the affirmative consent of an end user.

18  **SEC. 3. PROHIBITED CONDUCT.**

19      (a) IN GENERAL.—Except as provided in subsection

20  (e), it shall be unlawful for a controller to knowingly—

21       (1) use facial recognition technology to collect

22  facial recognition data, unless the controller—

23            (A) obtains from an end user affirmative

24  consent in accordance with subsection (b); and

1    (B) to the extent possible, if facial recogni-
2        tion technology is present, provides to the end
3        user—

4            (i) a concise notice that facial recogni-
5        tion technology is present, and, if contex-
6        tually appropriate, where the end user can
7        find more information about the use of fa-
8        cial recognition technology by the con-
9        troller; and

10           (ii) documentation that includes gen-
11       eral information that explains the capabili-
12       ties and limitations of the facial recogni-
13       tion technology in terms that end users are
14       able to understand;

15   (2) use the facial recognition technology to dis-
16   criminate against an end user in violation of applica-
17   ble Federal or State law;

18   (3) repurpose facial recognition data for a pur-
19   pose that is different from those presented to the
20   end user under paragraph (1)(A); or

21   (4) share the facial recognition data with an
22   unaffiliated third party without affirmative consent
23   that is separate from the affirmative consent re-
24   quired under paragraph (1)(A).

25   (b) CONSENT.—

1    (1) IN GENERAL.—When obtaining affirmative

2  consent, a controller shall make available to an end

3  user a notice that describes the specific practices of

4  the processor in terms that end users are able to un-

5  derstand regarding the collection, storage, and use

6  of facial recognition data, including—

7         (A) the reasonably foreseeable purposes, or

8      examples, for which the processor collects and

9      shares information derived from facial recogni-

10      tion technology or uses facial recognition tech-

11      nology;

12         (B) the data retention and deidentification

13      practices of the processor; and

14         (C) if the controller offers the ability to re-

15      view, correct, or delete information derived from

16      facial recognition technology, the process to ac-

17      complish such actions.

18    (2) PROCESSOR REQUIREMENT.—If the proc-

19  essor and controller are not the same entity, the

20  processor shall make easily accessible to controllers

21  the information required under paragraph (1).

22    (3) CONDITIONING SERVICE ON CONSENT PRO-

23  HIBITED.—If the use of facial recognition technology

24  is not necessary for a service, no controller may—

1     (A) condition the service on consent by an

2    end user to waive privacy rights; or

3     (B) terminate or refuse the service as a di-

4    rect consequence of refusal by the end user to

5    provide affirmative consent to the covered enti-

6    ty.

7 (c) REVIEW.—A controller, and the processor if appli-

8 cable, shall employ meaningful human review prior to

9 making any final decision based on the output of facial

10 recognition technology if the final decision—

11   (1) may result in a reasonably foreseeable and

12  material physical or financial harm to an end user;

13  or

14   (2) may be unexpected or highly offensive to a

15  reasonable end user.

16 (d) APPLICATION PROGRAMMING INTERFACE.—A

17 covered entity that makes a facial recognition technology

18 available as an online service shall make available an ap-

19 plication programming interface to enable at least 1 third

20 party that is legitimately engaged in independent testing

21 to conduct reasonable tests of the facial recognition tech-

22 nology for accuracy and bias.

23 (e) EXCEPTIONS.—

1 (1) IN GENERAL.—Except as provided in para-

2 graph (2), subsections (a)(1) and (b) shall not apply

3 to controllers that use—

4 (A) an application that—

5 (i) is a product or service designed for

6 personal file management or photo or video

7 sorting or storage if the facial recognition

8 technology is not used for unique personal

9 identification of a specific individual;

10 (ii) involves identification of public

11 figures for journalistic media created for

12 public interest;

13 (iii) involves identification of public

14 figures in copyrighted material for theat-

15 rical release; or

16 (iv) is used if there is an emergency

17 involving imminent danger or risk of death

18 or serious physical injury to an individual;

19 or

20 (B) facial recognition data to determine

21 whether an end user has given affirmative con-

22 sent if the controller immediately and perma-

23 nently destroys the facial recognition data after

24 determining that the end user has not given af-

25 firmative consent.

1      (2) SECURITY APPLICATIONS.—Subsections

2     (a)(1)(A) and (b) shall not apply to controllers that

3     use an application that is a security application.

4      (3) RULE OF CONSTRUCTION.—Nothing in

5     paragraph (1)(B) may be construed to authorize the

6     mass scanning of faces in spaces where end users do

7     not have a reasonable expectation that facial rec-

8     ognition technology is being used on them.

9 **SEC. 4. ENFORCEMENT.**

10   (a) UNFAIR OR DECEPTIVE ACT OR PRACTICE.—A

11 violation of section 3 shall be treated as a violation of a

12 rule defining an unfair or deceptive act or practice pre-

13 scribed under section 18(a)(1)(B) of the Federal Trade

14 Commission Act (15 U.S.C. 57a(a)(1)(B)).

15   (b) POWERS OF COMMISSION.—

16      (1) IN GENERAL.—The Federal Trade Commis-

17     sion shall enforce this Act in the same manner, by

18     the same means, and with the same jurisdiction as

19     though all applicable terms and provisions of the

20     Federal Trade Commission Act (15 U.S.C. 41 et

21     seq.) were incorporated into and made a part of this

22     Act.

23      (2) PRIVILEGES AND IMMUNITIES.—Any person

24     who violates section 3 shall be subject to the pen-

25     alties and entitled to the privileges and immunities

1 provided in the Federal Trade Commission Act (15

2 U.S.C. 41 et seq.).

3 (c) ENFORCEMENT BY STATES.—

4 (1) IN GENERAL.—If the attorney general of a

5 State has reason to believe that an interest of the

6 residents of the State has been or is being threat-

7 ened or adversely affected by a practice that violates

8 section 3, the attorney general of the State may, as

9 parens patriae, bring a civil action on behalf of the

10 residents of the State in an appropriate district

11 court of the United States to obtain appropriate re-

12 lief.

13 (2) RIGHTS OF COMMISSION.—

14 (A) NOTICE TO COMMISSION.—

15 (i) IN GENERAL.—Except as provided

16 in clause (iii), the attorney general of a

17 State, before initiating a civil action under

18 paragraph (1), shall provide written notifi-

19 cation to the Commission that the attorney

20 general intends to bring such civil action.

21 (ii) CONTENTS.—The notification re-

22 quired under clause (i) shall include a copy

23 of the complaint to be filed to initiate the

24 civil action.

1                (iii) EXCEPTION.—If it is not feasible

2                for the attorney general of a State to pro-

3                vide the notification required under clause

4                (i) before initiating a civil action under

5                paragraph (1), the attorney general shall

6                notify the Commission immediately upon

7                instituting the civil action.

8           (B) INTERVENTION BY COMMISSION.—The

9      Commission may—

10               (i) intervene in any civil action

11               brought by the attorney general of a State

12               under paragraph (1); and

13               (ii) upon intervening—

14                   (I) be heard on all matters aris-

15                ing in the civil action; and

16                   (II) file petitions for appeal of a

17                decision in the civil action.

18      (3) INVESTIGATORY POWERS.—Nothing in this

19    subsection may be construed to prevent the attorney

20    general of a State from exercising the powers con-

21    ferred on the attorney general by the laws of the

22    State to conduct investigations, to administer oaths

23    or affirmations, or to compel the attendance of wit-

24    nesses or the production of documentary or other

25    evidence.

1      (4) VENUE; SERVICE OF PROCESS.—

2          (A) VENUE.—Any action brought under

3      paragraph (1) may be brought in—

4          (i) the district court of the United

5      States that meets applicable requirements

6      relating to venue under section 1391 of

7      title 28, United States Code; or

8          (ii) another court of competent juris-

9      diction.

10          (B) SERVICE OF PROCESS.—In an action

11      brought under paragraph (1), process may be

12      served in any district in which—

13          (i) the defendant is an inhabitant,

14      may be found, or transacts business; or

15          (ii) venue is proper under section

16      1391 of title 28, United States Code.

17      (5) ACTIONS BY OTHER STATE OFFICIALS.—

18          (A) IN GENERAL.—In addition to a civil

19      action brought by an attorney general under

20      paragraph (1), any other officer of a State who

21      is authorized by the State to do so may bring

22      a civil action under paragraph (1), subject to

23      the same requirements and limitations that

24      apply under this subsection to civil actions

25      brought by attorneys general.

1           (B) SAVINGS PROVISION.—Nothing in this

2         subsection may be construed to prohibit an au-

3         thorized official of a State from initiating or

4         continuing any proceeding in a court of the

5         State for a violation of any civil or criminal law

6         of the State.

**SEC. 5. REGULATIONS.**

8     (a) REGULATIONS.—Not later than 180 days after

9 the date of enactment of this Act, the Federal Trade Com-

10 mission, in consultation with the National Institute of

11 Standards and Technology, shall promulgate regulations,

12 in accordance with section 553 of title 5, United States

13 Code—

14         (1) describing data security, minimization, and

15         retention standards to be met at a minimum by

16         processors;

17         (2) defining what is harmful and highly offen-

18         sive under paragraphs (1) and (2) of section 3(c);

19         and

20         (3) expanding the list of exceptions described in

21         section 3(e) in cases where it is impossible for a con-

22         troller to obtain affirmative consent from, or provide

23         notice to, end users.

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

4     (1) the size of the processor;

5     (2) the complexity of the offerings of the proc-
6     essor; and

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

9 **SEC. 6. RELATION TO STATE LAWS.**

10 (a) IN GENERAL.—This Act shall not be construed
11 as superseding, altering, or affecting any statute, regula-
12 tion, order, or interpretation in effect in any State, except
13 to the extent that such statute, regulation, order, or inter-
14 pretation is inconsistent with the provisions of this Act,
15 and then only to the extent of the inconsistency.

16 (b) GREATER PROTECTION UNDER STATE LAW.—
17 For purposes of this Act, a State statute, regulation,
18 order, or interpretation is not inconsistent with the provi-
19 sions of this subtitle if the protection such statute, regula-
20 tion, order, or interpretation affords any person is greater
21 than the protection provided under this Act, as determined
22 by the Federal Trade Commission.

23 **SEC. 7. RELATION TO OTHER PRIVACY AND SECURITY**
24        **LAWS.**

25 Nothing in this Act may be construed to—

1        (1) modify, limit, or supersede the operation of

2    any privacy or security provision in any other Fed-

3    eral or State law (including regulations); or

4        (2) limit the authority of the Commission under

5    any other provision of law.

6 **SEC. 8. EFFECTIVE DATE.**

7    This Act shall take effect on the date that is 180 days

8 after the date of enactment of this Act.

○