

116TH CONGRESS
1ST SESSION

S. 2878

To limit the use of facial recognition technology by Federal agencies, and
for other purposes.

IN THE SENATE OF THE UNITED STATES

NOVEMBER 14, 2019

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

A BILL

To limit the use of facial recognition technology by Federal
agencies, 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 “Facial Recognition
5 Technology Warrant Act of 2019”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

8 (1) AGENCY.—The term “agency” has the
9 meaning given the term in section 551 of title 5,
10 United States Code.

1 (2) COVERED COURT ORDER.—The term “cov-
2 ered court order” means a court order obtained in
3 accordance with rule 41 of the Federal Rules of
4 Criminal Procedure and in connection with the in-
5 vestigation of an offense for which an order could be
6 sought under section 2516 of title 18, United States
7 Code.

8 (3) FACIAL RECOGNITION TECHNOLOGY.—The
9 term “facial recognition technology” means tech-
10 nology that analyzes facial features and is used for
11 the unique personal identification of individuals in
12 still or video images.

13 (4) ONGOING SURVEILLANCE.—The term “on-
14 going surveillance”—

15 (A) means the utilization of facial recogni-
16 tion technology to engage in a sustained effort
17 to track the physical movements of an identified
18 individual through 1 or more public places
19 where such movements occur over a period of
20 time greater than 72 hours, whether in real
21 time or through application of such technology
22 to historical records; and

23 (B) does not include instances where facial
24 recognition technology is utilized for a single
25 identification or attempted identification of an

1 individual, if no subsequent attempt is made to
2 track that individual's movement in real time or
3 through the use of historical records after the
4 individual has been identified.

5 **SEC. 3. LIMITATION ON USE OF FACIAL RECOGNITION**
6 **TECHNOLOGY.**

7 (a) IN GENERAL.—Subject to subsection (b), an offi-
8 cer or employee of an agency may not use facial recogni-
9 tion technology to engage in ongoing surveillance of an
10 individual or group of individuals in a public space, un-
11 less—

12 (1) the use of the facial recognition technology
13 is in support of a law enforcement activity; and

14 (2)(A) a covered court order has been obtained
15 to allow the use of facial recognition technology for
16 ongoing surveillance of the individual or group of in-
17 dividuals; or

18 (B) an investigative or law enforcement offi-
19 cer—

20 (i) reasonably determines that exigent cir-
21 cumstances and compelling law enforcement
22 needs make it impractical to obtain a covered
23 court order;

1 (ii) reasonably determines that there are
 2 grounds for which a covered court order could
 3 be obtained under subparagraph (A); and

4 (iii) causes an application for a covered
 5 court order to be made in accordance with sub-
 6 paragraph (A) not later than 48 hours after the
 7 use of facial recognition technology to engage in
 8 ongoing surveillance.

9 (b) REQUIREMENT.—If an application for a covered
 10 court order made under subsection (a)(2)(B) is denied, the
 11 use of facial recognition technology shall terminate at the
 12 time of the denial.

13 (c) DURATION OF ORDERS.—

14 (1) IN GENERAL.—Subject to paragraph (2), a
 15 covered court order may only authorize ongoing sur-
 16 veillance until the date on which the objective of the
 17 order is satisfied, except that such order may not
 18 authorize ongoing surveillance for a period of longer
 19 than 30 days.

20 (2) REQUIREMENT.—The 30-day period de-
 21 scribed in paragraph (1) shall begin on the earlier
 22 of—

23 (A) the date on which the agency begins to
 24 use facial recognition technology; or

1 (B) the date that is 10 days after the
2 court order is issued.

3 (3) EXTENSION.—A court may grant an exten-
4 sion of the 30-day period described in paragraph (1)
5 if the extension satisfies the requirements of sub-
6 section (a)(2)(A) and such extension may last not
7 longer than 30 days.

8 (d) MINIMIZATION REQUIREMENT.—Any use of fa-
9 cial recognition technology pursuant to a covered court
10 order shall be conducted in such a way as to minimize
11 the acquisition, retention, and dissemination of informa-
12 tion about the individuals other than those for whom there
13 was probable cause to seek the covered court order ob-
14 tained under subsection (a)(2)(A).

15 (e) MOTION TO SUPPRESS.—

16 (1) IN GENERAL.—Except as provided in para-
17 graph (2), any aggrieved individual who has been
18 the subject of ongoing surveillance using facial rec-
19 ognition technology, in any trial, hearing, or pro-
20 ceeding in or before any court, department, officer,
21 agency, regulatory body, or other authority of the
22 United States, a State, or a political subdivision
23 thereof, may move to suppress information directly
24 obtained through the use of facial recognition tech-

nology, or evidence derived therefrom, in violation of this section, on the grounds that—

(A) the information was unlawfully obtained;

(B) the order of authorization or approval under which the information was obtained is insufficient on its face; or

(C) the use of facial recognition technology was not used in conformity with the order of authorization or approval.

(2) EXCEPTION.—Evidence obtained through the use of facial recognition technology in violation of this section shall not be suppressed under paragraph (1) if the evidence was acquired by an officer or an employee of an agency with an objectively reasonable belief that the use of facial recognition technology was in compliance with this section.

(3) REQUIREMENT.—A motion described in paragraph (1) shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the individual was not aware of the grounds of the motion. If the motion is granted, the information directly obtained through the use of facial recognition technology, or evidence derived

1 therefrom, shall be treated as having been obtained
2 in violation of this section.

3 (4) INSPECTION OF INFORMATION.—The judge,
4 upon the filing of a motion under this subsection by
5 the aggrieved individual, may in his or her discretion
6 make available to the aggrieved individual or counsel
7 of the aggrieved individual for inspection such por-
8 tions of the information or evidence derived there-
9 from as the judge determines to be in the interests
10 of justice.

11 (5) APPEAL.—In addition to any other right to
12 appeal, the United States shall have the right to ap-
13 peal from an order granting a motion to suppress
14 made under this subsection, or the denial of an ap-
15 plication for an order of approval, if the United
16 States attorney shall certify to the judge or other of-
17 ficial granting such motion or denying such applica-
18 tion that the appeal is not taken for purposes of
19 delay. Such appeal shall be taken within 30 days
20 after the date the order was entered and shall be
21 diligently prosecuted.

22 (6) LIMITATION.—The remedies and sanctions
23 described in this subsection with respect to the use
24 of facial recognition technology are the only judicial

1 remedies and sanctions for nonconstitutional viola-
 2 tions of this section involving such technology.

3 (f) FOREIGN INTELLIGENCE INFORMATION.—Noth-
 4 ing in this section shall be construed to affect the use of
 5 facial recognition technology to engage in ongoing surveil-
 6 lance connected with the acquisition of foreign intelligence
 7 information, as defined in section 101(e) of the Foreign
 8 Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(e)).

9 **SEC. 4. REPORTS ON GOVERNMENT USE OF FACIAL REC-**
 10 **OGNITION TECHNOLOGY.**

11 (a) REPORT BY JUDGE.—Not later than 30 days
 12 after issuance of a covered court order under section
 13 3(a)(2)(A) or an extension thereof under section 3(c)(3),
 14 or the denial of such a warrant or extension, the issuing
 15 or denying judge shall report to the Administrative Office
 16 of the United States Courts—

17 (1) the fact that a warrant or extension was ap-
 18 plied for;

19 (2) the fact that the warrant or extension was
 20 granted as applied for, was modified, or was denied;

21 (3) the period of time for which the warrant ap-
 22 proves the use of facial recognition technology, and
 23 the number and duration of any extensions; and

24 (4) the offense specified in the warrant or ap-
 25 plication.

1 (b) REPORTS.—Beginning 1 year after the date of
2 enactment of this Act, and not later than September 30
3 of each year thereafter, the Director of the Administrative
4 Office of the United States Courts shall transmit to the
5 Committee on the Judiciary of the Senate and the Com-
6 mittee on the Judiciary of the House of Representatives,
7 and make available to the public, a full and complete re-
8 port summarizing the data required to be filed with the
9 Administrative Office under subsection (a), including—

10 (1) the number of applications for covered court
11 orders and extensions authorizing delayed notice;

12 (2) the number of covered court orders and ex-
13 tensions granted or denied during the preceding fis-
14 cal year;

15 (3) for each covered court order or extension
16 granted—

17 (A) the period of time for which the war-
18 rant approves the use of facial recognition tech-
19 nology, and the number and duration of any ex-
20 tensions;

21 (B) the offense specified in the covered
22 court order or application, or extension of an
23 order;

24 (C) the identity of the applying investiga-
25 tive or law enforcement officer and agency mak-

1 ing the application and the person authorizing
2 the application; and

3 (D) the nature of the facilities or cameras
4 from which the data analyzed by facial recogni-
5 tion technology came from;

6 (4) a general description of the identifications
7 made under a covered court order or extension, in-
8 cluding—

9 (A) the approximate nature and frequency
10 of use of the facial recognition technology;

11 (B) the approximate number of persons
12 who were subjected to analysis using the facial
13 recognition technology; and

14 (C) the approximate nature, amount, and
15 cost of the manpower and other resources dur-
16 ing the use of the facial recognition technology;
17 and

18 (5) the number of misidentifications, including
19 any arrest of an individual that does not result in
20 charges being entered against the individual, made
21 based upon information directly obtained through
22 the use of facial recognition technology, or evidence
23 derived therefrom.

24 (c) REGULATIONS.—The Director of the Administra-
25 tive Office of the United States Courts, in consultation

1 with the Attorney General, may issue guidance regarding
2 the content and form of the reports required to be filed
3 under subsection (a).

4 **SEC. 5. HUMAN REVIEW AND TESTING.**

5 (a) HUMAN REVIEW OF FACIAL RECOGNITION TECH-
6 NOLOGY.—An agency shall require a trained officer to ex-
7 amine the output or recommendation of any facial recogni-
8 tion system before the agency investigates or otherwise
9 interacts with an individual identified by the system in
10 connection with a covered court order issued under section
11 3(a)(2)(A) or in connection with an emergency under sec-
12 tion 3(a)(2)(B).

13 (b) TESTING.—The head of each agency, in consulta-
14 tion with the Director of the National Institute of Stand-
15 ards and Technology, shall establish testing procedures re-
16 garding all facial recognition technology systems used by
17 the agency, including a process to—

18 (1) periodically undertake independent tests of
19 the performance of the system in typical operational
20 conditions;

21 (2) identify relative performance across dif-
22 ferent subpopulations, including error rates when
23 the system is tested across subpopulations, alone
24 and in combination with, different skin tones, ages,
25 and genders; and

1 (3) review such tests and take action to improve
2 the accuracy of the system across subpopulations
3 upon a finding indicating there are disparate error
4 rates when the system is tested across subpopula-
5 tions.

○