

117TH CONGRESS
2D SESSION

H. R. 9061

To regulate law enforcement use of facial recognition technology, and for
other purposes.

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 29, 2022

Mr. LIEU (for himself, Ms. JACKSON LEE, Ms. CLARKE of New York, and Mr. GOMEZ) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Committee on Science, Space, and Technology, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To regulate law enforcement use of facial recognition
technology, 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 Act
5 of 2022”.

6 **SEC. 2. INELIGIBILITY FOR CERTAIN FUNDS.**

7 In the case of a State or unit of local government
8 that received a grant award under subpart 1 of part E

1 of title I of the Omnibus Crime Control and Safe Streets
2 Act of 1968 (42 U.S.C. 3750 et seq.), if the State or unit
3 of local government fails to substantially to comply with
4 the requirements under this Act for a fiscal year, the At-
5 torney General shall reduce the amount that would other-
6 wise be awarded to that State or unit of local government
7 under such grant program in the following fiscal year by
8 15 percent.

9 **SEC. 3. DEFINITIONS.**

10 In this Act:

11 (1) **ARREST PHOTO DATABASE.**—The term “ar-
12 rest photo database” means a database populated
13 primarily by booking or arrest photographs or photo-
14 graphs of persons encountered by an investigative or
15 law enforcement officer.

16 (2) **CANDIDATE LIST.**—The term “candidate
17 list” means the top images that a facial recognition
18 system determines to most closely match a probe
19 image.

20 (3) **DERIVED.**—The term “derived” means that
21 a Federal or State government would not have pos-
22 sessed the information or evidence but for the use of
23 facial recognition, regardless of any claim that the
24 information or evidence is attenuated from such rec-
25 ognition, and would inevitably have been discovered

1 or obtained the information or evidence through
2 other means.

3 (4) FACIAL RECOGNITION.—The term “facial
4 recognition” means an automated or semi-automated
5 process that assists in identifying or verifying an in-
6 dividual or captures information about an individual
7 based on the physical characteristics of an individ-
8 ual’s face, head or body, or that uses characteristics
9 of an individual’s face, head or body, to infer emo-
10 tion, associations, activities, or the location of an in-
11 dividual.

12 (5) FACE SURVEILLANCE.—The term “face sur-
13 veillance” means the use of facial recognition with
14 real-time or stored video footage to track, observe,
15 or analyze the movements, behavior, data, or actions
16 of an individual or groups of individuals.

17 (6) ILLEGITIMATELY OBTAINED INFORMA-
18 TION.—The term “illegitimately obtained informa-
19 tion” means personal data or information that was
20 obtained—

21 (A) in a manner that violates Federal,
22 State, or Tribal law;

23 (B) in a manner that violates a service
24 agreement between a provider of an electronic
25 communication service to the public or a pro-

vider of a remote computing service and customers or subscribers of that provider;

(C) in a manner that is inconsistent with the privacy policy of a provider described in subparagraph (B), if applicable;

(D) by deceiving a person whose information was obtained;

(E) through the unauthorized access of an electronic device or online account;

(F) in violation of a contract, court settlement, or other binding legal agreement; or

(G) from unlawful or unconstitutional practices by any government official or entity.

(7) INVESTIGATIVE OR LAW ENFORCEMENT OFFICER.—The term “investigative or law enforcement officer” means—

(A) any officer of a State or a political subdivision thereof, or of the United States, who is empowered by law to conduct investigations of or to make arrests for civil or criminal offenses or violations of Federal or State law and any attorney authorized by law to prosecute or participate in the prosecution of such offenses; and

1 (B) does not include any officer, employee,
2 or contractor of a State department of motor
3 vehicles.

4 (8) LAW ENFORCEMENT AGENCY.—The term
5 “law enforcement agency” means any agency of the
6 United States authorized to engage in or supervise
7 the prevention, detection, investigation, or prosecu-
8 tion of any violation of civil or criminal law.

9 (9) PROBE IMAGE.—The term “probe image”
10 means an image of a person that is searched against
11 a database of known, identified persons or an un-
12 solved photo file.

13 (10) PROSECUTOR.—The term “prosecutor”
14 means the principal prosecuting attorney of a State
15 or any political subdivision thereof and any attorney
16 for the Government (as such term is defined for the
17 purposes of the Federal Rules of Criminal Proce-
18 dure).

19 (11) OPERATIONAL TESTING.—The term “oper-
20 ational testing” means testing that evaluates a com-
21 plete facial recognition system as it is used in the
22 field, including measuring false positive and false
23 negative error rates for field uses of the system on
24 operational or operationally representative data and
25 under the environmental conditions and technical

product settings and configurations typically used,
as well as assessing the variability of system use by
different users.

(12) REFERENCE PHOTO DATABASE.—The
term “reference photo database” means a database
populated with photos of individuals that have been
identified, including databases composed of driver’s
licenses, passports, or other documents made or
issued by or under the authority of the United
States Government, a State, a political subdivision
thereof, databases operated by third parties, and ar-
rest photo databases.

(13) STATE.—The term “State” means each
State of the United States, the District of Columbia,
the Commonwealth of Puerto Rico, the Virgin Is-
lands, American Samoa, Guam, and the Northern
Mariana Islands.

TITLE I—USE OF FACIAL REC- OGNITION BY LAW ENFORCE- MENT

SEC. 101. FACIAL RECOGNITION.

(a) REFERENCE PHOTO DATABASES.—

(1) IN GENERAL.—An investigative or law en-
forcement officer may only use or request facial rec-
ognition in conjunction with a reference photo data-

1 base pursuant to an order issued under subsection
2 (b) and the emergencies and exceptions under sub-
3 section (c).

4 (2) MAINTENANCE.—

5 (A) IN GENERAL.—Beginning on 180 days
6 after the date of the enactment of this Act, and
7 every six months thereafter, with respect to an
8 arrest photo database used in conjunction with
9 facial recognition, the custodian of such arrest
10 photo database shall remove from such data-
11 base all photos of each person who—

12 (i) has not attained 18 years of age;

13 (ii) has been released without a
14 charge;

15 (iii) has been released after charges
16 are dropped or dismissed; or

17 (iv) was acquitted of the charged of-
18 fense.

19 (B) RULE OF CONSTRUCTION.—Nothing in
20 this paragraph shall be construed to prohibit an
21 investigative or law enforcement officer from
22 using a database for other investigative proce-
23 dures, such as finger printing, and shall only
24 apply to the use of a reference photo database
25 for the use of facial recognition.

1 (3) PROCEDURES.—Any agency responsible for
2 maintaining and operating an arrest photo database
3 shall establish procedures to ensure compliance with
4 paragraph (3).

5 (b) ORDERS.—

6 (1) APPROVAL.—An application for a warrant
7 to use a reference photo database may not be sub-
8 mitted for consideration by a court unless the head
9 of a law enforcement agency (or a designee) ap-
10 proves such an application.

11 (2) AUTHORITY.—Except as provided by sub-
12 section (d), the principal prosecutor of a State or
13 any political subdivision thereof and any attorney for
14 the Government (as such term is defined for the
15 purposes of the Federal Rules of Criminal Proce-
16 dure), may make an application to a court of com-
17 petent jurisdiction for, in conformity with paragraph
18 (3), an order authorizing the use of facial recogni-
19 tion in conjunction with a reference photo database
20 within the jurisdiction of that judge.

21 (3) APPLICATION.—Except as provided in sub-
22 section (e), a court of competent jurisdiction may
23 issue an order authorizing the use of facial recogni-
24 tion in conjunction with a reference photo database

1 if a prosecutor submits an application to that court
2 that establishes the following:

3 (A) The identity of the investigative or law
4 enforcement officer making the application, and
5 the officer authorizing the application.

6 (B) As full and complete a description as
7 possible of the person that the officer seeks to
8 identify.

9 (C) The photos or video portraying the
10 person that will be used to search the reference
11 photo database.

12 (D) Any details regarding other investiga-
13 tive measures taken to identify such person and
14 an explanation for why such measures failed or
15 are reasonably unlikely to succeed.

16 (E) Any other investigative procedures to
17 identify such person have been tried and failed
18 or are reasonably unlikely to succeed.

19 (F) Probable cause to believe that such
20 person has committed or is committing a par-
21 ticular offense or offenses enumerated in sec-
22 tion 3559(c)(2)(F) of title 18, United States
23 Code.

24 (4) CONTENTS OF ORDER.—The order de-
25 scribed in this paragraph shall include the following:

1 (A) All information required to be included
2 in the application pursuant to such paragraph
3 (3).

4 (B) A prohibition on the use, for purposes
5 of a search of a reference photo database, other
6 than pursuant to another order under this Act,
7 of any photo or video not specifically listed in
8 the order.

9 (C) A time period within which the search
10 shall be made not more than 7 days, and after
11 which no such search may be made, except pur-
12 suant to another order under this Act.

13 (D) The authority under which the search
14 is to be made.

15 (5) NOTICE TO THE PUBLIC.—

16 (A) IN GENERAL.—Each State department
17 of motor vehicles shall post notices in con-
18 spicuous locations at each department office,
19 make written information available to all appli-
20 cants at each office, and provide information on
21 the department website regarding State inves-
22 tigative or law enforcement officers' searches of
23 driver's license and ID photos through facial
24 recognition. The notices, written information,
25 and online information must describe how offi-

1 cers use and access facial recognition in crimi-
2 nal investigations.

3 (B) LANGUAGE REQUIREMENT.—Notices
4 required under subparagraph (A) shall be post-
5 ed, as necessary and reasonable, in Spanish or
6 any language common to a significant portion
7 of the department’s customers, if they are not
8 fluent in English. The department shall provide
9 translations of the poster and an electronic link
10 that leads to the department’s website upon re-
11 quest.

12 (6) CONFORMING AMENDMENTS.—Section 2721
13 of title 18, United States Code, is amended—

14 (A) in subsection (a)—

15 (i) in paragraph (1), by striking the
16 “or” at the end;

17 (ii) in paragraph (2), by striking the
18 period at the end and inserting “; or”; and

19 (iii) by inserting after paragraph (2)
20 the following:

21 “(3) a department operated facial recognition
22 system, except as provided in subsection (e) of this
23 section.”;

24 (B) in subsection (b)(1), by inserting be-
25 fore the period at the end the following: “but if

1 the personal information or highly restricted
2 personal information to be disclosed is a per-
3 son’s photograph to be used or enrolled in a law
4 enforcement facial recognition system, only on a
5 case-by-case basis that does not involve the bulk
6 transfer of persons’ photographs to a State or
7 Federal law enforcement agency or a qualified
8 third party entity that will allow law enforce-
9 ment to access those photographs for the pur-
10 poses of facial recognition”; and

11 (C) by adding at the end the following:

12 “(e) LAW ENFORCEMENT ACCESS TO FACIAL REC-
13 OGNITION SYSTEMS.—A State department of motor vehi-
14 cles, and any officer, employee, or contractor thereof, may
15 make available a department-operated facial recognition
16 system to a State or Federal law enforcement agency, or
17 perform searches of such a system on behalf of the agency,
18 only pursuant to an order issued under section 101 of the
19 ‘facial recognition Act of 2022’.”.

20 (c) EMERGENCIES AND EXCEPTIONS.—

21 (1) INITIAL USE.—Notwithstanding subsections
22 (a) and (b), an investigative or law enforcement offi-
23 cer may use or request facial recognition in conjunc-
24 tion with a reference photo database—

1 (A) to assist in identifying any person who
2 is deceased, incapacitated or otherwise phys-
3 ically unable of identifying himself, or the vic-
4 tim of a crime, whom the officer determines, in
5 good faith, cannot be identified through other
6 means;

7 (B) to assist in identifying a person whom
8 the officer believes, in good faith, is the subject
9 of an alert through an AMBER Alert commu-
10 nications network, as that term is used in sec-
11 tion 301 of the Prosecutorial Remedies and
12 Other Tools to end the Exploitation of Children
13 Today Act of 2003 (34 U.S.C. 20501);

14 (C) to assist in identifying any person who
15 has been lawfully arrested, during the process
16 of booking that person after an arrest or during
17 that person's custodial detention; or

18 (D) to assist in identifying any person—
19 (i) if the appropriate prosecutor deter-
20 mines that an emergency situation exists—

21 (I) that involves immediate dan-
22 ger of death or serious physical injury
23 to any person; or

24 (II) that requires the use of fa-
25 cial recognition in conjunction with a

1 reference photo database to occur be-
2 fore an order authorizing such use
3 can, with due diligence, be obtained;
4 and

5 (ii) there are grounds upon which an
6 order could be entered under this section
7 to authorize such use.

8 (2) SUBSEQUENT AUTHORIZATION.—If an in-
9 vestigative or law enforcement officer uses facial rec-
10 ognition pursuant to paragraph (1)(D), the pros-
11 ecutor shall apply for an order approving the use
12 under subsection (b) within 12 hours after the use
13 occurred. The use shall immediately terminate when
14 the application for approval is denied, or in the ab-
15 sence of an application, within 12 hours. In cases
16 where an order is not obtained or denied, the officer
17 shall destroy all information obtained as a result of
18 the search.

19 (3) AFFIDAVIT REQUIRED.—With respect to use
20 of facial recognition pursuant to paragraph (1)(D),
21 an appropriate prosecutor shall submit an affidavit
22 to the court identifying specific details on why they
23 believe that an emergency situation under clause (i)
24 exists.

1 (d) STATE LAW PRESERVED.—The authorities pro-
2 vided by subsections (b) and (c) do not authorize access
3 reference photo databases maintained by a State, or a po-
4 litical subdivision of a State, unless State law expressly
5 and unambiguously authorizes an investigative or law en-
6 forcement officer to—

7 (1) access driver’s license and identification
8 document photos; and

9 (2) use facial recognition to conduct searches of
10 those photos.

11 **SEC. 102. CIVIL RIGHTS AND CIVIL LIBERTIES.**

12 (a) IN GENERAL.—An investigative or law enforce-
13 ment officer may not—

14 (1) use facial recognition to create a record de-
15 scribing how any individual exercises rights guaran-
16 teed by the Constitution, including free assembly, as-
17 sociation, and speech;

18 (2) rely on actual or perceived race, ethnicity,
19 national origin, religion, disability, gender, gender
20 identity, or sexual orientation in selecting which per-
21 son to subject to facial recognition, except when
22 there is trustworthy information, relevant to the lo-
23 cality and time frame, in the context of a particular
24 area and for a particular period of time, that links
25 a person with a particular characteristic described in

1 this subsection to an identified criminal incident or
2 scheme; or

3 (3) use facial recognition to enforce the immi-
4 gration laws of the United States or share facial rec-
5 ognition data with other agencies for the purposes of
6 enforcing the immigration laws of the United States.

7 (b) PROHIBITION ON USE WITH BODY CAMERAS.—
8 Any investigative or law enforcement officer may not use
9 or request facial recognition in conjunction with any image
10 obtained from a body camera worn by that or any other
11 officer, dashboard camera, or any aircraft camera, includ-
12 ing a drone.

13 (c) PROHIBITION ON CERTAIN FACIAL RECOGNI-
14 TION.—Any investigative or law enforcement officer may
15 not use or request facial recognition for the purpose of
16 face surveillance.

17 (d) ENSURING CORROBORATION AND PREVENTING
18 OVER RELIANCE ON MATCHES.—A facial recognition
19 match may not be the sole basis upon which probable
20 cause is established for a search, arrest, or other law en-
21 forcement action. Any investigative and law enforcement
22 officers using information obtained from the use of facial
23 recognition shall examine results with care and consider
24 the possibility that matches could be inaccurate.

1 (e) PROHIBITION ON ILLEGITIMATELY OBTAINED IN-
2 FORMATION.—An investigative or law enforcement office
3 may not use facial recognition in conjunction with a data-
4 base that contains illegitimately obtained information.

5 **SEC. 103. LOGGING OF SEARCHES.**

6 A law enforcement agency whose investigative or law
7 enforcement officers use facial recognition shall log its use
8 of the facial recognition to the extent necessary to comply
9 with the public reporting and audit requirements of sec-
10 tions 104 and 105 of this Act.

11 **SEC. 104. REPORTING.**

12 (a) STATE REPORTING REQUIRED.—

13 (1) STATE JUDICIARY.—Not later than the last
14 day of the first January after the date of the enact-
15 ment of this Act, and each January thereafter, each
16 State judge who has issued a court order authorizing
17 or approving facial recognition in conjunction with a
18 reference photo database shall report to a State
19 agency (as determined by the chief executive of the
20 State) the following information:

21 (A) The number of orders or extensions
22 was applied for.

23 (B) Whether the order or extension was
24 issued pursuant to section 101(b) or section
25 102(c).

1 (C) Whether the order or extension was
2 granted as applied for, was modified, or was de-
3 nied.

4 (D) The offense specified in the order or
5 application, or extension of an order.

6 (E) The identity of the applying investiga-
7 tive or law enforcement officer and agency mak-
8 ing the application and the person authorizing
9 the application.

10 (F) For orders issued pursuant to section
11 101(c), the reference photo database that was
12 searched.

13 (2) PROSECUTORS.—Not later than the last day
14 of the first January after the date of the enactment
15 of this Act, and each January thereafter, each State
16 prosecutor, or a prosecutor of a political subdivision
17 thereof, who has requested a court order authorizing
18 or approving facial recognition in conjunction with a
19 reference photo database shall report to a State
20 agency (as determined by the chief executive of the
21 State) the following information with respect to the
22 use of facial recognition in conjunction with an ref-
23 erence photo database:

24 (A) The number of such searches run.

1 (B) The offenses that those searches were
2 used to investigate, and for each offense, the
3 number of searches run.

4 (C) The arrests that such searches contrib-
5 uted to, and the offenses for which the arrests
6 were made, disaggregated by race, ethnicity,
7 gender, and age.

8 (D) The number of convictions that such
9 searches contributed to and the offenses for
10 which the convictions were obtained,
11 disaggregated by race, ethnicity, gender, and
12 age.

13 (E) The number of motions to suppress
14 made with respect to those searches, and the
15 number granted or denied.

16 (F) The types and names of databases that
17 were used and the number of photos removed
18 with respect to arrest photo databases that
19 were confirmed to have been removed in accord-
20 ance with this section.

21 (3) REPORT TO BUREAU OF JUSTICE ASSIST-
22 ANCE.—Not later than 90 days after such report is
23 submitted under paragraph (1), and annually there-
24 after, the State agency shall report the information

1 collected under paragraph (1) to the Director of the
2 Bureau of Justice Assistance.

3 (4) REPORT TO ADMINISTRATIVE OFFICE OF
4 THE UNITED STATES COURTS.—Not later than 90
5 days after such report is submitted under paragraph
6 (2), and annually thereafter, the State agency shall
7 report the information collected under paragraph (2)
8 to the Director of the Administrative Office of the
9 United States Courts.

10 (b) FEDERAL REPORTING REQUIRED.—Not later
11 than the last day of the first January after the date of
12 the enactment of this Act, and each January thereafter—

13 (1) each Federal judge who has issued a court
14 order authorizing or approving facial recognition in
15 conjunction with a reference photo database shall
16 submit to the Director of the Administrative Office
17 of the United States Courts a report including the
18 information under subparagraphs (A) through (F) of
19 subsection (a)(1); and

20 (2) and a Federal prosecutor who requested
21 such order, shall submit to the Director of the Ad-
22 ministrative Office of the United States Courts a re-
23 port including the information under subparagraphs
24 (A) through (G) of subsection (a)(2).

1 (c) PUBLIC REPORTING.—In June of each year the
2 Director of the Administrative Office of the United States
3 Courts shall release to the public, post online, and trans-
4 mit to the Congress a full and complete report concerning
5 the use of facial recognition in conjunction with reference
6 photo databases, including the information reported to the
7 Director pursuant to subsections (a) and (b).

8 (d) RULES.—The Director of the Bureau of Justice
9 Assistance and the Director of the Administrative Office
10 of the United States Courts shall issue rules with respect
11 to the content and form of the reports required to be filed
12 under subsections (a) through (c) of this section and sec-
13 tions 105 and 106 of this Act.

14 **SEC. 105. AUDITS.**

15 (a) FEDERAL LEVEL AUDIT.—

16 (1) IN GENERAL.—Any Federal law enforce-
17 ment agency whose investigative or law enforcement
18 officers use facial recognition, regardless of whether
19 they use a system operated by that agency or an-
20 other agency, shall annually submit data with re-
21 spect to their use of facial recognition for audit by
22 the Government Accountability Office to prevent and
23 identify misuse and to ensure compliance with sec-
24 tions 101, 102, and 103 of this Act, including—

1 (A) a summary of the findings of the
2 audit, including the number and nature of vio-
3 lations identified; and

4 (B) information about the procedures used
5 by the law enforcement agency to remove arrest
6 photos from databases in accordance with this
7 Act.

8 (2) SUSPENSION.—

9 (A) IN GENERAL.—If a violation is uncov-
10 ered by the audit conducted under paragraph
11 (1), the Federal law enforcement agency shall
12 cease using facial recognition until such time
13 that all violations have been corrected.

14 (B) PUBLIC NOTICE.—If use of facial rec-
15 ognition is suspended pursuant to subparagraph
16 (A), the Federal law enforcement agency shall
17 notify the public of such suspension.

18 (b) STATE LEVEL AUDIT.—

19 (1) IN GENERAL.—Any State or local law en-
20 forcement agency whose investigative or law enforce-
21 ment officers use facial recognition, regardless of
22 whether they use a system operated by that agency
23 or another agency, shall annually submit data with
24 respect to their use of facial recognition to an inde-
25 pendent State agency (as determined by the chief ex-

1 ecutive of the State) to prevent and identify misuse
2 and to ensure compliance with sections 101, 102,
3 and 103 of this Act. Such independent State agency
4 shall report—

5 (A) a summary of the findings of the
6 audit, including the number and nature of vio-
7 lations identified, to Director of the Administra-
8 tive Office of the United States Courts, and
9 subsequently release that information to the
10 public and post it online;

11 (B) information about the procedures used
12 by the law enforcement agency to remove arrest
13 photos from databases in accordance with this
14 section; and

15 (C) any violations identified by the inde-
16 pendent State agency.

17 (2) SUSPENSION.—

18 (A) IN GENERAL.—If a violation is uncov-
19 ered by the audit conducted under paragraph
20 (1), the State or local law enforcement agency
21 shall cease using facial recognition until such
22 time that all violations have been corrected.

23 (B) PUBLIC NOTICE.—If use of facial rec-
24 ognition is suspended pursuant to subparagraph

1 (A), the State or local law enforcement agency
2 shall notify the public of such suspension.

3 (c) DISAGGREGATED DATA.—Data collected pursu-
4 ant to subsection (a) or (b) shall, when feasible, be col-
5 lected in a manner that allows such data to be
6 disaggregated by race, ethnicity, gender, and age.

7 **SEC. 106. ACCURACY AND BIAS TESTING.**

8 (a) BENCHMARK TESTING.—No investigative or law
9 enforcement officers may use a facial recognition system
10 or information derived from it unless that system is annu-
11 ally submitted to the National Institute of Standards and
12 Technology’s benchmark facial recognition test for law en-
13 forcement to determine—

14 (1) the accuracy of the system; and

15 (2) whether the accuracy of the system varies
16 significantly on the basis of race, ethnicity, gender
17 or age.

18 (b) BENCHMARK TESTING FOR NEW SYSTEMS.—No
19 investigative or law enforcement officers may begin using
20 a new facial recognition system or information derived
21 from it unless that system is first submitted to inde-
22 pendent testing to determine—

23 (1) the accuracy of the system; and

1 (2) whether the accuracy of the system varies
2 significantly on the basis of race, ethnicity, gender,
3 or age.

4 (c) PROHIBITION.—Any investigative or law enforce-
5 ment officer may not use facial recognition that has not
6 achieved a sufficiently high level of accuracy, including in
7 terms of overall accuracy and variance on the basis of
8 race, ethnicity, gender, or age, as determined by the Na-
9 tional Institute of Standards and Technology, on its an-
10 nual benchmark test for law enforcement use.

11 (d) OPERATIONAL TESTING.—No investigative or law
12 enforcement agencies may use a facial recognition system
13 or information derived from it unless that system is annu-
14 ally submitted to operational testing conducted by an inde-
15 pendent entity, in accordance with National Institute of
16 Standards and Technology’s training protocol for oper-
17 ational testing, to determine—

18 (1) the accuracy of the system;

19 (2) the impact of human reviewers on system
20 accuracy; and

21 (3) whether the accuracy of the system varies
22 significantly on the basis of race, ethnicity, gender,
23 or age.

24 (e) REPORTING.—A summary of the findings of the
25 tests required by subsection (a) or (d) shall be submitted

1 to the Director of the Administrative Office of the United
2 States Courts and posted on the internet website of the
3 Administrative Office of the United States Courts.

4 (f) RULEMAKING REQUIRED.—The Assistant Attor-
5 ney General of the Department of Justice Civil Rights Di-
6 vision shall issue a rule that establishes what is a suffi-
7 ciently high level of accuracy for a facial recognition sys-
8 tem used by law enforcement, including in terms of overall
9 accuracy and variance on the basis of race, ethnicity, gen-
10 der, and age. The Assistant Attorney General of the De-
11 partment of Justice Civil Rights Division shall consult
12 with outside experts in civil rights, civil liberties, racial
13 justice, data privacy, bioethics, law enforcement, public de-
14 fense, and forensic science and other relevant areas of ex-
15 pertise in drafting the proposed rule.

16 (g) EFFECTIVE DATE.—This section shall take effect
17 18 months after the date of enactment of this Act.

18 **SEC. 107. ENFORCEMENT.**

19 (a) SUPPRESSION.—In the case that the use of facial
20 recognition has occurred, no results from the use and no
21 evidence derived therefrom may be received in evidence in
22 any trial, hearing, or other proceeding in or before any
23 court, grand jury, department, officer, agency, regulatory
24 body, legislative committee, or other authority of the
25 United States, a State, or a political subdivision thereof

1 if the use of facial recognition violated this Act or if the
2 use was conducted in an emergency under section 101 and
3 the officer or agency did not subsequently obtain an order
4 for that use as required under such section.

5 (b) ADMINISTRATIVE DISCIPLINE.—If a court or law
6 enforcement agency determines that an investigative or
7 law enforcement officer has violated any provision of this
8 Act, and the court or agency finds that the circumstances
9 surrounding the violation raise serious questions about
10 whether or not the officer acted intentionally with respect
11 to the violation, the agency shall promptly initiate a pro-
12 ceeding to determine whether disciplinary action against
13 the officer is warranted.

14 (c) CIVIL ACTION.—

15 (1) IN GENERAL.—Any person who is subject to
16 identification or attempted identification through fa-
17 cial recognition in violation of this Act may bring a
18 civil action in the appropriate court to recover such
19 relief as may be appropriate from the investigative
20 or law enforcement officer or the State or Federal
21 law enforcement agency which engaged in that viola-
22 tion.

23 (2) RELIEF.—In an action under this sub-
24 section, appropriate relief includes—

1 (A) such preliminary and other equitable
2 or declaratory relief as may be appropriate;

3 (B) damages under paragraph (3) and pu-
4 nitive damages in appropriate cases; and

5 (C) a reasonable attorney's fee and other
6 litigation costs reasonably incurred.

7 (3) COMPUTATION OF DAMAGES.—The court
8 may assess as damages whichever is the greater of—

9 (A) any profits made with respect to the
10 violation suffered by the plaintiff; or

11 (B) \$50,000 for each violation.

12 (4) DEFENSE.—A good faith reliance on—

13 (A) a court warrant or order, a grand jury
14 subpoena, a legislative authorization, or a statu-
15 tory authorization; or

16 (B) a good faith determination that section
17 101 permitted the conduct complained of,
18 is a complete defense against any civil action
19 brought under this Act.

20 (5) LIMITATION.—A civil action under this sec-
21 tion may not be commenced later than two years
22 after the date upon which the claimant first has a
23 reasonable opportunity to discover the violation.

24 (d) CIVIL ACTION FOR DISPARATE IMPACT.—An in-
25 dividual may bring a civil action when use of facial rec-

1 ognition or face surveillance by a law enforcement agency,
2 or any technological element, criteria, method, or design
3 feature thereof acting individually or in concert, results
4 in disparate treatment or adverse impact against an indi-
5 vidual or class of individuals on the basis of race, ethnicity,
6 gender, or age.

7 **SEC. 108. NOTICE REQUIREMENT.**

8 (a) NOTICE REQUIREMENT.—A law enforcement
9 agency that uses facial recognition to attempt to identify
10 an individual who is arrested shall, at minimum, provide
11 to the individual—

12 (1) a notice of—

13 (A) the name the law enforcement agency
14 that operated the facial recognition system
15 used; and

16 (B) the name of the database, if any, that
17 was used to identify the individual; and

18 (2) a copy of—

19 (A) the order that authorized the use of fa-
20 cial recognition;

21 (B) accuracy or bias reports required
22 under this Act;

23 (C) each probe image that was used by the
24 agency;

1 (D) any modifications made to the probe
2 image;

3 (E) the candidate list, in rank order, pro-
4 duced by the facial recognition system; and

5 (F) any other police documentation related
6 to the use of facial recognition in the law en-
7 forcement investigation.

8 (b) LANGUAGE REQUIREMENT.—The information re-
9 quired under subsection (a) shall be provided to such indi-
10 vidual in an appropriate language for such individual if
11 the individual is not fluent or literate in English.

12 **TITLE II—CERTAIN REQUIRE-**
13 **MENTS AND LIMITATIONS ON**
14 **FACIAL RECOGNITION SYS-**
15 **TEMS AND RESEARCH**

16 **SEC. 201. NATIONAL INSTITUTE FOR STANDARDS AND**
17 **TECHNOLOGY ASSISTANCE.**

18 (a) IN GENERAL.—The National Institute of Stand-
19 ards and Technology (hereinafter in this section referred
20 to as “NIST”) shall—

21 (1) develop best practices for law enforcement
22 agencies to evaluate the accuracy and fairness of
23 their facial recognition systems;

24 (2) develop and offer an ongoing benchmark fa-
25 cial recognition test for law enforcement that—

1 (A) conducts evaluations of actual algo-
2 rithms used by law enforcement agencies;

3 (B) uses the types of probe images, includ-
4 ing in terms of quality, actually used by law en-
5 forcement agencies in its testing;

6 (C) evaluates algorithms on larger data-
7 bases that reflect the size of databases actually
8 used by law enforcement; and

9 (D) evaluates whether the accuracy of a fa-
10 cial recognition algorithm varies on the basis of
11 race, ethnicity, gender, or age and assessments
12 of bias in facial recognition systems;

13 (3) develop an operational testing protocol that
14 independent testers and law enforcement agencies
15 may implement for annual operational testing to de-
16 termine—

17 (A) the accuracy of the facial recognition
18 system;

19 (B) the impact of human reviewers on fa-
20 cial recognition system accuracy; and

21 (C) whether the accuracy of the facial rec-
22 ognition system varies significantly on the basis
23 of race, ethnicity, gender, or age; and

24 (4) study and develop training standards for
25 human operators reviewing the results of facial rec-

1 ognition searches to ensure accuracy and prevent
2 bias.

3 (b) AUTHORIZATION OF APPROPRIATIONS.—There is
4 authorized to be appropriated to the National Institute of
5 Standards and Technology to carry out subsection (a)
6 \$5,000,000 for each of the fiscal years 2023 through
7 2026.

8 **SEC. 202. RULE OF CONSTRUCTION WITH RESPECT TO**
9 **STATE AND LOCAL PRIVACY PROTECTIONS.**

10 (a) RULE OF CONSTRUCTION.—Nothing in this Act
11 shall be construed to preempt concurrent or more strin-
12 gent limitations on the use of facial recognition, or any
13 other privacy, civil rights, and civil liberties laws and rules,
14 by the Federal Government, a State, or a political subdivi-
15 sion of a State.

16 (b) USE OF FACIAL RECOGNITION.—Nothing in this
17 Act shall be construed to authorize the use of facial rec-
18 ognition by a State, or a political subdivision of a State,
19 unless the laws of that State or political subdivision ex-
20 pressly and unambiguously authorizes such use.

21 **SEC. 203. POLICY ON USE OF FACIAL RECOGNITION SYS-**
22 **TEMS REQUIRED.**

23 Not later than 90 days after the date of the enact-
24 ment of this Act, each agency covered by this statute shall
25 establish and make publicly available on the internet

1 website of such agency a policy governing the agency's use
2 of facial recognition systems to ensure investigative or law
3 enforcement officer compliance with the requirements of
4 this Act.

5 **SEC. 204. LIMITATION ON LIABILITY.**

6 A State shall not be immune under the eleventh
7 amendment to the Constitution of the United States from
8 an action in Federal or State court of competent jurisdic-
9 tion for a violation of this Act. In any action against a
10 State for a violation of the requirements of this Act, rem-
11 edies (including remedies both at law and in equity) are
12 available for such a violation to the same extent as such
13 remedies are available for such a violation in an action
14 against any public or private entity other than a State.

○